Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution

De Terwangne , Cécile; Van Gyseghem, Jean-Marc

Published in:
Vie privée et données à caractère personnel

Publication date:
2013

Document Version
le PDF de l'éditeur

CHAPITRE 3.2.
ANALYSE DÉTAILLÉE DE LA LOI DE PROTECTION DES DONNÉES ET DE SON ARRÊTÉ ROYAL D'EXÉCUTION

Cécile DE TERWANGNE
Jean-Marc VAN GYSEGHEM

Ainsi qu'il a été signalé ci-dessus, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[1] a fait l'objet d'un remaniement considérable lors de la transposition en droit belge de la directive 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[2], également évoquée *supra*. Ce remaniement s'est effectué par le biais de la loi du 11 décembre 1998[3].

On retrouve parfois dans la pratique des mentions de cette loi de 1998 comme étant celle de référence en la matière. Or cette deuxième loi a pour objet de modifier la première et n'a pas d'autonomie propre. Nous évoquerons donc toujours dans les pages qui suivent la « loi du 8 décembre 1992 », étant entendu qu'elle est analysée

1. Sur cette loi, voy. les analyses et commentaires suivants : M.-H. BOULANGER, C. DE TERWANGNE et TH. LÉONARD, « La protection de la vie privée à l'égard des traitements de données à caractère personnel. La loi du 8 décembre 1992 », *J.T.*, 1993, pp. 369 à 388 ; J. DUMORTIER (éd.) et F. ROBBEN (éd.), *Persoonsgegevens en privacybescherming. Commentaar op de wet tot bescherming van de persoonlijke levenssfeer*, Brugge, die Keure, 1995.
2. Pour un commentaire détaillé de la directive, voy. M.-H. BOULANGER, C. DE TERWANGNE, TH. LÉONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, pp. 121 à 179.
3. Loi du 11 décembre 1998 transposant la directive (CE) 95/46 du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B.*, 3 février 1999. Pour une analyse et un commentaire approfondis de la nouvelle loi, voy. D. DE BOT, *Verwerking van persoonsgegevens*, Antwerpen, Kluwer, 2001 ; C. DE TERWANGNE, « La nouvelle loi belge de protection des données à caractère personnel », *in* P. TABATONI (dir.), *La protection de la vie privée dans la société d'information. Cahier des Sciences morales et politiques*, Paris, PUF, 2002, pp. 91 à 109, disponible sur le site de l'Académie des Sciences morales et politiques, http://www.asmp.fr/travaux/gpw_internetvieprivee.htm ; C. DE TERWANGNE et S. LOUVEAUX, « Protection des données à caractère personnel : application en Belgique de la directive européenne », *in Actualités du droit des technologies de l'information et de la communication*, coll. Formation permanente CUP, Liège, vol. 45, février 2001, pp. 5 à 34 ; J. DHONT et Y. POULLET, « Data protection Belgium – An analysis of the new law », *C.L.S.R.*, 2000, vol. 16, n° 1, pp. 5 et s. ; B. DOCQUIR, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, pp. 151 et s. ; J. DUMORTIER, « De nieuwe wetgeving over de verwerking van persoonsgegevens », *Recente ontwikkelingen in informatica- en telecommunicatierecht*, Brugge, die Keure, 1999, pp. 73 à 103 ; TH. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, pp. 377 et s. ; S. LOUVEAUX et F. DE BROUWER, « Protection des données à caractère personnel. Vers une nouvelle loi belge », *Ubiquité*, 1998, pp. 83 à 99 ; M. VAN OVERSTRAETEN et S. DEPRÉ, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, pp. 665 à 701 ; V. VERBRUGGEN, *Les Codes commentés. Protection des données à caractère personnel (loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)*, Bruxelles, Larcier, 2011, 283 p.

dans sa version modifiée de 1998, augmentée des apports et modifications apparus subséquemment. Des amendements ou ajouts ont en effet été adoptés depuis le renouvellement de la loi. Parmi ces apports ultérieurs, généralement mineurs ou marginaux, le plus marquant consiste en l'introduction de comités sectoriels au sein de l'organe de contrôle national, la Commission de la protection de la vie privée. On relèvera d'emblée que ces comités sectoriels sont un concept tout à fait propre à la Belgique.

La loi du 8 décembre 1992 dans sa version révisée est entrée en vigueur le 1er septembre 2001, selon le prescrit de l'arrêté royal d'exécution du 13 février 2001[1].

Cette loi étant le fruit de la transposition en droit national de la directive européenne 95/46, il doit être tenu compte, pour son application et son interprétation, des indications données par les organes juridictionnels de l'Union européenne au travers de leur jurisprudence portant sur cette directive. La jurisprudence des juridictions belges de même que la pratique développée par la Commission de la protection de la vie privée sont bien évidemment à prendre également en considération pour déterminer les contours des dispositions légales. L'on doit également noter que la Cour constitutionnelle a considéré que *"(...) La Cour peut examiner si le législateur a respecté les obligations internationales qui découlent des dispositions invoquées de [la directive 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données] et de la convention n° 108 [du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel] auxquelles la Loi précitée du 8 décembre 1992 et ses modifications ultérieures donnent exécution. Ces obligations forment un ensemble indissociable des garanties qui sont reproduites à l'article 22 de la Constitution."*[2] En d'autres termes, la Cour constitutionnelle considère que la loi du 8 décembre 1992 forme un tout par rapport aux normes européennes de l'Union européenne et du Conseil de l'Europe.

1. Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001. C. DE TERWANGNE et S. LOUVEAUX, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.*, 2001, pp. 457 à 469.
2. C.C. (29/2010), 18 mars 2010, www.const-court.be ; nous soulignons.

1. Objet de la loi

1.1. Intitulé de la loi

La loi de 1992 est intitulée « loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel », ce qui a conduit à son appellation abrégée courante « loi vie privée » (LVP).

Or cette appellation est trompeuse car il s'agit davantage d'une loi de protection des données à caractère personnel que d'une loi garantissant la vie privée dans le sens classique de celle-ci qui est un concept différent et plus restrictif même s'il y est intimement lié. Comme on le verra dans le point éclairant la notion de « donnée à caractère personnel » ci-dessous, la portée de cette loi dépasse largement la sphère intime dans laquelle on cantonne souvent la vie privée.

Il est impératif, pour ceux qui ont à appliquer la loi, d'être conscients de la nouvelle dimension que la notion de « vie privée » a acquise[1]. La vie privée, dans ce contexte, rappelons-le, ne doit pas se comprendre comme limitée à un ensemble d'informations personnelles ou d'images que l'on souhaite garder cachées, ou à des actions que l'on mène derrière un mur, à l'abri des regards et des interférences. Elle est à entendre comme autodétermination, comme autonomie et, plus particulièrement, comme autonomie informationnelle, c'est-à-dire l'autonomie dans la détermination des conditions d'usage et de communication des informations qui se rapportent à soi-même[2]. La vie privée, c'est, en ce sens, la maîtrise par chacun de son image informationnelle.

Conserver une approche « classique » de la vie privée peut conduire à une mauvaise interprétation de l'objet de la loi du 8 décembre 1992. C'est ce qui est arrivé à un juge qui, se basant sur l'intitulé de la loi, a estimé que celle-ci n'était pas d'application à un cas qui mettait en cause des données relatives aux prestations professionnelles d'un travailleur, de telles données ne relevant pas, aux yeux de ce juge, de la vie privée. Cette approche est bien évidemment erronée.

---

1. Voy. l'introduction du présent ouvrage.
2. Voy. H. BURKERT, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *D.I.T.*, 1985, pp. 8 à 16 ; C. DE TERWANGNE, « Le rapport de la vie privée à l'information », *in* E. MONTERO (dir.), *Droit des technologies de l'information. Regards prospectifs*, Cahier du CRID, n° 16, Bruxelles, Bruylant, 1999, p. 144 ; J. DHONT, « Le traitement des données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, 1/2000, pp. 322 et s. ; TH. LÉONARD et Y. POULLET, « Les libertés comme fondement de la protection des données nominatives », *in* F. RIGAUX, *La vie privée : une liberté parmi les autres ?*, Travaux de la Faculté de droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s. ; M. PARISSE et V. VERBRUGGEN, « Secret professionnel et vie privée : les traitements de données à caractère personnel (relatives à la santé) couvertes par le secret professionnel » , *R.D.T.I.*, 2006, pp. 29 et s. ; M. VAN OVERSTRAETEN et S. DEPRÉ, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, pp. 669 et s., spéc. pp. 685 à 690. P. WASCHMANN, « Le droit au secret de la vie privée », *in* FR. SUDRE (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruxelles, Bruylant, 2005, pp. 119 à 155.

Il eût mieux valu sans doute ne pas faire référence à la vie privée dans l'intitulé de la loi, mais bien plutôt à la protection des données à caractère personnel ou à la protection des personnes à l'égard du traitement des données à caractère personnel.

Il est à noter que cette référence à la « vie privée » se retrouve dans l'appellation de l'autorité de contrôle qui, en Belgique, est nommée « Commission de la protection de la vie privée » alors que cette commission n'est compétente qu'en matière de protection des données à caractère personnel. Cela génère un flux de questions relatives à la « vie privée » de la part des citoyens, auxquelles la Commission n'est pas à même de répondre.

À l'inverse, la Région wallonne et la Fédération Wallonie-Bruxelles viennent de se doter d'un organe de contrôle à leur niveau et ont veillé à ne pas choisir une appellation évoquant la vie privée. Elles ont appelé cette commission commune, « Commission Wallonie-Bruxelles de contrôle des échanges de données » (CCED, en abrégé), pour éviter toute ambiguïté[1].

1.2. Protection des droits et libertés parmi lesquels le droit à la vie privée

Alors que, dans la première version de la loi de 1992, l'article 2 stipulait que « toute personne physique a droit au respect de sa vie privée lors du traitement des données à caractère personnel qui la concerne », cette disposition énonce depuis 1998 que, « [l]ors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée ».

Depuis ce changement de texte[2] apparu à la suite de la transposition de la directive 95/46, il est bien clair que l'objet de la loi non seulement n'est pas à entendre comme protection de la vie privée au sens traditionnel, mais n'est pas non plus limité à la protection de la seule vie privée. La loi vise à la protection de l'ensemble des libertés et droits fondamentaux des individus, parmi lesquels leur droit à la vie privée[3]

1. Décret wallon du 10 juillet 2013 portant assentiment à l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.*, 23.07.2013, et décret de la Communauté française portant assentiment à l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative, *M.B.*, 23.07.2013. Par ailleurs, cet accord de coopération du 23 mai 2013 a créé une Banque-carrefour d'échange de données (BCED, en abrégé).Les Gouvernements wallon et de la Fédération Wallonie-Bruxelles ont créé, via l'accord de coopération du 21 février 2013 (*M.B.*, 28.06.2013 et *M.B.*, 28.06.2013), le service **e**-Wallonie-Bruxelles Simplification (eWBS). Ce service eWBS est rattaché auprès du Secrétariat général du Service public de Wallonie et auprès du Secrétariat général du Ministère de la Fédération Wallonie-Bruxelles.
2. On peut cependant se demander si cela n'a pas instillé une certaine ambiguïté.
3. Voy. Y. POULLET, « La protection des données : entre libertés, droits subjectifs et intérêts légitimes », *in Liber amicorum Paul Martens*, Bruxelles, Larcier, 2007, pp. 133 à 150 ; M. VAN OVERSTRAETEN et S. DEPRÉ, *op. cit.*, pp. 669 et s.

Il est vrai que la protection des données à caractère personnel met en cause la protection d'autres droits et libertés que le droit au respect de la vie privée, tels que la liberté de se déplacer, la liberté de s'assurer, de se loger, de trouver un emploi, de s'informer et de s'exprimer en toute transparence, etc. Ainsi, la création de bases de données permettant un profilage des individus peut amener à discriminer ceux-ci lors de la recherche d'un logement, de la demande d'une couverture d'assurance ou de la recherche d'informations. De même, le remplacement progressif des modes de paiement traditionnels par des paiements par le biais de cartes de crédit émises par des sociétés commerciales se trouvant en situation oligopolistique met ces sociétés en mesure d'analyser toutes les utilisations de la carte et, en conséquence, de surveiller les activités des détenteurs de carte[1].

2. Définitions

2.1. La notion de « données à caractère personnel »

L'article 1er, § 1er, de la LVP donne de la « donnée à caractère personnel » une définition textuellement reprise de la directive européenne en la matière. Par cette expression il faut entendre « toute information concernant une personne physique identifiée ou identifiable », cette dernière étant appelée la « personne concernée »[2].

La loi s'applique donc à l'égard de n'importe quelle information pourvu que celle-ci puisse être rattachée directement ou indirectement à un individu[3].

1. Voy. ce qui est exposé dans l'introduction du présent ouvrage. Également C. DE TERWANGNE et J.-PH. MOINY, *Les lacunes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) face aux développements technologiques*, Rapport pour le Conseil de l'Europe, Strasbourg, novembre 2010, pp. 4 et 5, disponible à l'adresse http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports_and_studies_fr.asp.
2. Voy. les éclaircissements apportés sur cette notion cardinale par le Groupe européen de protection des données de l'article 29 (ci-après « Groupe de l'article 29 »), avis 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel, *WP* 136.
3. Voy. les développements consacrés à cette notion dans le chapitre 1er du présent ouvrage, dans la section portant sur « La Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et les concepts fondamentaux de la protection des données ».

2.1.1. Les informations visées

Tous types d'informations

Ainsi qu'on l'a déjà dit, la notion de « données à caractère personnel » englobe n'importe quel type d'informations : informations privées, publiques, professionnelles ou commerciales, informations objectives ou subjectives[1].

La notion couvre les *informations privées*, intimes, mais également les *informations* communément qualifiées de **« publiques »** parce que librement accessibles dans des registres publics tels l'annuaire téléphonique[2].

La Cour de justice de l'Union européenne a eu l'occasion, dans son arrêt *Satamedia*[3], de clarifier le point de l'inclusion des *informations rendues publiques* dans le champ d'application de la directive 95/46 (et, partant, des lois nationales transposant cette dernière). La Cour a noté que la solution – qui est en fait celle de la loi finlandaise en cause dans l'affaire soumise à la Cour – d'une dérogation générale en faveur d'informations publiées viderait largement la directive de son sens, puisqu'il suffirait de publier des données pour les faire échapper à la protection établie par ce texte[4]. Pour la Cour, ce n'est pas parce que des données ont été diffusées, c'est-à-dire portées à la connaissance ou rendues accessibles à un nombre indéfini de personnes, qu'elles ne bénéficient plus d'une protection. En d'autres mots, il n'est pas question de dépouiller de toute protection des données dès lors qu'elles sont rendues publiques d'une quelconque façon, que ce soit notamment sur Internet ou dans un journal[5].

Entrent aussi dans le champ de la notion de donnée à caractère personnel les *données relatives à la vie professionnelle* d'un individu ou *à ses activités commerciales*. On relève en ce sens que « n'exclut pas l'application de la loi, le fait que les données soient relatives à un commerçant, un indépendant, une profession libérale ou l'administrateur d'une société »[6]. Il a été reconnu par le Tribunal de première instance de l'Union européenne que les noms et prénoms des fonctionnaires européens et des personnes figurant sur les listes de réserve des concours de recrutement organisés par l'Union européenne constituaient des données à caractère personnel[7]. Le Tribu-

1. Sur le fait que les données à caractère personnel ne sont pas limitées aux informations relatives à la vie privée, voy. M. Van Overstraeten et S. Depré, *op. cit.*, p. 677 ; O. De Schutter, « Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel », *Rev. trim. dr. h.*, 2001, pp. 150 et s.
2. Dans sa première version, la loi excluait de son champ d'application les données faisant l'objet d'une publicité en vertu d'une disposition légale ou réglementaire et les données dont la personne à laquelle elles se rapportent assurait la publicité, pour autant que le traitement effectué sur ces données respectât les finalités de cette publicité (ancien art. 3, § 2). On était donc légitimé à parler de « données publiques », pas ou peu protégées.
3. C.J.C.E., 16 décembre 2008 (Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et satamedia oy), C-73/07.
4. Point 48 de l'arrêt préc.
5. Point 49 de l'arrêt préc.
6. J.-Ph. Moiny et J.-M. Van Gyseghem, « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T.I.*, 2009, p. 83.
7. T.P.I., 7 juillet 2011 (Gregorio Valero Jordana c. Commission), T-161/04, point 91.

nal a réfuté par là la thèse du requérant qui soutenait que l'information selon laquelle une personne est fonctionnaire ne peut pas être considérée comme relevant de sa vie privée[1]. Pour savoir si l'on est en présence de données à caractère personnel, il ne s'agit, en effet, pas de déterminer si une information relève ou non de la vie privée mais seulement d'établir si l'information se rapporte à une personne identifiée ou identifiable. L'on voit donc bien que la protection des données à caractère personnel dépasse le simple cadre de la vie privée.

Les noms et prénoms des personnes ayant participé à une réunion de travail figurant sur le procès-verbal de la réunion ont aussi été considérés comme des données à caractère personnel[2].

Le Tribunal de première instance de Bruxelles a spécifié que, « par données à caractère personnel, il faut comprendre toutes les informations qui concernent une personne physique quel que soit le secteur plus spécialisé dans lequel elles s'inscrivent ». Ce qui a amené le tribunal à considérer comme telles les informations relatives à la solvabilité d'une des parties au litige, malgré le fait que ces informations ont aussi une nature commerciale et professionnelle.[3]

La liste des données à caractère personnel est donc particulièrement longue et variée. Il peut s'agir de données contenues dans un répertoire d'adresses, professionnel ou non, ou dans une liste de clients, ou encore d'un numéro de plaque de voiture, de données bibliographiques, de l'identification des parties, des juges et des plaideurs dans les décisions de jurisprudence, des résultats scolaires d'un élève, du numéro de compte bancaire, d'un *log*, ainsi que l'a considéré la Cour d'appel de Liège dans un arrêt du 22 octobre 2009[4], etc. Le Conseil d'état a estimé, dans un arrêt du 27 octobre 2005, qu'« un test d'haleine entraîne la collecte d'une donnée à caractère personnel »[5].

Des *données « matérielles »* portant sur des « choses », mais pouvant être reliées à des individus identifiés, sont aussi à considérer comme des données à caractère personnel. C'est ce qu'indiquent l'avis de la Commission de la protection de la vie privée portant sur le numéro de châssis et autres données d'identification du véhicule[6] ou celui sur les données cadastrales[7] ou encore l'avis concernant les images

1. *Idem*, point 60. Voy. C. GAYREL, « Chronique de jurisprudence en droit des technologies de l'information (2009-2011). Libertés et société de l'information. Cour de Justice de l'Union européenne, Tribunal de Première Instance et Tribunal de la Fonction publique européenne », *R.D.T.I.*, n^{os} 48 et 49, 2012, p. 93.
2. C.J.U.E. (Gr. Ch.), 29 juin 2010 (Commission c. The Bavarian Lager Co. Ltd.), C-28/08, point 86.
3. Civ. Bruxelles, 12 avril 1995, n° rôle 9553A, http://jure.juridat.just.fgov.be.
4. Liège (7^{e} ch.), 22 octobre 2009, *R.D.T.I.*, n° 38/2010, pp. 95 et s.
5. C.E., 27 octobre 2005, n^{o} 150.861 http://www.raadvst-consetat.be.
6. Commission de la protection de la vie privée (ci-après, « C.P.V.P. »), avis Car Pass 15/2006 du 14 juin 2006 relatif au projet d'arrêté royal réglant la collaboration à l'association chargée de l'enregistrement du kilométrage des véhicules.
7. Comité sectoriel pour l'Autorité fédérale, délibération AF n° 02/2012 du 9 février 2012 concernant la demande du SPF Intérieur, Direction générale Sécurité civile, d'accéder à certaines données cadastrales (Documentation patrimoniale – SPF Finances) dans le cadre de la réforme des services de secours.

satellites[1]. La valeur d'une maison rattachée au patrimoine de son propriétaire ou les données de localisation géographique de taxis associées à leurs chauffeurs relèvent de la même manière de la catégorie des données à caractère personnel[2].

À travers l'ordinateur dans lequel ils sont glissés, les « **cookies** »[3] visent à informer sur l'utilisateur de cet ordinateur[4]. Dans son avis sur les aspects de la protection des données liés aux moteurs de recherche, le Groupe de l'article 29 conclut que, « lorsqu'un cookie contient un identifiant d'utilisateur unique, celui-ci est clairement une donnée à caractère personnel. L'utilisation de « cookies » persistants ou de dispositifs similaires comportant un identifiant d'utilisateur unique permet de pister les utilisateurs d'un ordinateur donné, même en cas d'utilisation d'adresses IP dynamiques. Les données relatives au comportement qui sont générées par le recours à ces dispositifs permettent d'affiner encore les caractéristiques personnelles de la personne concernée. »

La notion de données à caractère personnel couvre enfin tant les données qui résultent d'éléments objectifs, vérifiables et contestables, que les *données subjectives* contenant une évaluation ou un jugement porté sur quelqu'un[5]. C'est ainsi le cas des données d'évaluation des employés, que cette évaluation soit exprimée sous forme de points, d'une échelle de valeurs ou par le biais d'autres paramètres d'évaluation[6]. Les données subjectives que sont les évaluations de la fiabilité d'une personne en matière de crédit ou les pronostics en matière d'assurance entrent également dans la définition des données à caractère personnel.

Toutes formes d'informations

Les données à caractère personnel peuvent prendre n'importe quelle forme, que ce soit celle d'un texte *écrit*, d'un *graphique*, d'images ou de son[7].

1. C.P.V.P., avis 26/2006 du 12 juillet 2006 concernant l'utilisation d'images satellites afin de dépister et de constater des infractions aux normes urbanistiques.
2. Voy. les développements sur ces deux exemples par le Groupe de l'article 29, *WP* 136, préc., pp. 10 et 12.
3. Un *cookie* (aussi appelé *témoin de connexion*) est un petit fichier envoyé et enregistré sur le disque dur de l'ordinateur d'un internaute par le serveur gérant le site Web visité. Il contient des informations sur la navigation effectuée par l'internaute sur les pages de ce site.
4. N'entrent pas en considération ici les « *cookies* de session », soit des *cookies* dont la durée de vie est limitée à une session de navigation.
5. Groupe de l'article 29, avis 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel, *WP* 136, p. 7.
6. Groupe de l'article 29, Recommandation 1/2001 du 22 mars 2001 concernant les données d'évaluation des employés, *WP* 42.
7. Voy. également le considérant n°14 de la directive 95/46 : « considérant que, compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données ; ».

La jurisprudence a déjà pu à mainte occasion dire que des *images* d'individus sous forme de photographies ou de films vidéo peuvent être considérées comme des données à caractère personnel[1].

Les enregistrements de *voix* entrent également dans le champ de la notion.

Les informations contenues dans un dessin réalisé par une personne identifiée ou identifiable sont des données à caractère personnel[2].

Les *données biométriques*[3] sont également des données à caractère personnel. Il faut entendre par là « des propriétés biologiques, des aspects comportementaux, des caractéristiques physiologiques, des caractéristiques vivantes ou des actions reproductibles lorsque ces caractéristiques et/ou actions sont à la fois propres à cette personne physique et mesurables, même si les méthodes utilisées dans la pratique pour les mesurer techniquement impliquent un certain degré de probabilité »[4]. Entrent donc dans cette catégorie de données des caractéristiques d'ordre physique (les empreintes digitales, la rétine, l'iris, la structure faciale, la voix, la forme de l'oreille, la géométrie du contour de la main, le système veineux, l'odeur corporelle, etc.) ou comportemental (signature manuscrite, manière de frapper sur un clavier, démarche ou élocution particulières, etc.)[5].

Si les tissus humains ou matériel biologique d'origine humaine (sang, salive, cheveu…) ne sont pas en soi des données à caractère personnel, les informations issues de l'analyse de ces tissus le sont bien, elles. Les *données génétiques* (profils ADN) sont ainsi des données couvertes par la loi de 1992. Elles ont d'ailleurs été identifiées par la Cour européenne des droits de l'homme comme soulevant une préoccupation particulière au regard de la protection de la vie privée[6]. La Cour a relevé que les profils ADN contiennent une quantité importante de données à caractère personnel uni-

1. Voy. Corr. Bruxelles (51e ch.), 14 janvier 2002, *A.M.*, 2002, pp. 198 et s. ; Gand, 28 mars 2002, *T. Strafr.*, 2002, liv. 6, p. 329 ; Liège (6e ch.), 27 juin 2003, *R.D.T.I.*, 2004, n° 18, pp. 105 et s. ; Mons (1re ch.), 2 mai 2005, *J.L.M.B.*, 2005, p. 1057.
2. « À la suite d'un test neuropsychiatrique pratiqué sur une fillette dans le contexte d'une procédure judiciaire concernant sa garde, celle-ci fait un dessin représentant sa famille. Ce dessin fournit des informations sur l'état d'esprit de la fillette et ses sentiments envers différents membres de sa famille. Ces informations pourraient, en soi, être considérées comme des "informations à caractère personnel". Ce dessin révèle, en effet, des informations concernant cet enfant (sa santé mentale), mais aussi le comportement de son père ou de sa mère par exemple. En conséquence, les parents peuvent dans ce cas user de leur droit d'accéder à cet élément d'information spécifique. » (Groupe de l'article 29, *WP* 136, sur le concept de donnée à caractère personnel, préc., p. 7.)
3. Voy. Conseil de l'Europe, Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques (2005), CM(2005)43, Annexe II, disponible à l'adresse http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrie_2005.pdf. La biométrie y est présentée comme faisant référence à « des systèmes qui utilisent des caractéristiques physiques, physiologiques ou des éléments de comportement personnel mesurables afin de déterminer l'identité ou de vérifier l'identité alléguée d'un individu ». Voy. aussi C.P.V.P., avis n° 17 / 2008 du 9 avril 2008 relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes. La biométrie y est définie comme étant « la science des variations biologiques dont le but est de déterminer ou de vérifier l'identité d'un individu à l'aide de procédés s'appuyant sur des caractéristiques humaines distinctes et individuelles ». Également Groupe de l'article 29, avis 3/2012 du 27 avril 2012 sur l'évolution des technologies biométriques, *WP* 193.
4. Groupe de l'article 29, *WP* 136, sur le concept de donnée à caractère personnel, préc., p. 9.
5. Groupe de l'article 29, Document de travail sur la biométrie, adopté le 1er août 2003, *WP* 80.
6. Cour eur. D.H. (Gr. Ch.), arrêt S. et Marper c. Royaume-Uni, 4 décembre 2008, req. nos 30562/04 et 30566/04, § 75.

ques qui, même si objectives et irréfutables, permettent aux autorités d'aller bien au-delà d'une identification neutre (les profils ADN peuvent notamment être utilisés pour effectuer des recherches familiales en vue de découvrir les relations génétiques pouvant exister entre des individus). La préoccupation est d'autant plus grande que les données génétiques peuvent révéler des informations que l'individu ne souhaite peut-être pas lui-même connaître.

2.1.2. Les personnes concernées

Pour être qualifiées de données à caractère personnel, les informations doivent concerner une personne physique identifiée ou identifiable, appelée « personne concernée ».

La nationalité de cette personne n'a pas d'incidence sur la qualification de donnée à caractère personnel, pas plus que sa résidence. Ainsi, peu importe que les personnes concernées aient ou non la nationalité belge et qu'elles résident ou non en Belgique.

Personne physique et non personne morale

La définition reprise dans la loi de 1992 ne vise que les personnes *physiques* à l'exclusion des personnes morales. Cette limitation aux personnes physiques peut s'expliquer par le fait que la loi traite d'un droit fondamental qui, en tant que tel, est *a priori* l'attribut des personnes physiques, même s'il est reconnu aujourd'hui que les personnes morales bénéficient de la protection de certains droits fondamentaux compatibles avec leur nature[1]. Cependant, « quand de telles données reposent sur des données qui à leur tour concernent une personne physique, la [loi vie privée] peut s'appliquer »[2]. Cette assertion se dégage de l'affaire soumise au Tribunal de commerce de Courtrai dans laquelle la donnée en cause était l'information selon laquelle une personne physique avait été administratrice d'une personne morale[3].

Personne vivante et non décédée

La question de l'applicabilité de la législation de protection des données aux données concernant des personnes décédées a suscité de nombreuses interrogations

1. À titre d'illustration de cette reconnaissance, voy. notamment l'arrêt de la Cour d'appel de Bruxelles qui a considéré que « le droit au respect de la vie privée bénéficie aussi, dans une certaine mesure, aux personnes morales. Dès lors, il peut être admis que le droit au respect de la vie privée des personnes morales englobe la protection de leurs secrets d'affaires » (Bruxelles, 30 juin 2010, *J.L.M.B.*, 25/2011, p. 1184).
2. J.-Ph. Mony et J.-M. Van Gyseghem, « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T.I.*, 2009, p. 83 ; voy. également Comm. Courtrai (1re ch.), 19 juin 2003, *T.G.R.-T.W.V.R.*, 2007, liv. 2, p. 100, confirmé par Gent, 6 janvier 2005, *T.G.R.-T.W.V.R.*, liv. 2, 2007, pp. 92 et 93.
3. Comm. Courtrai (1re ch.), 19 juin 2003, préc.

et les prises de position ont varié tant parmi les auteurs de doctrine[1] que dans la jurisprudence de la Commission de la protection de la vie privée et des juridictions judiciaires[2]. À plusieurs reprises, la Commission de la protection de la vie privée s'est prononcée sur la situation des données après la mort de la personne concernée. À une position floue mêlant argumentation à partir de la protection de la vie privée et analyse impliquant la protection des données[3], a succédé, dans un second temps, une position en faveur de l'application de la loi du 8 décembre 1992 aux données concernant des personnes décédées. Dans son avis relatif aux archives de l'État[4], la Commission s'est prononcée dans les termes suivants : « [...] Les documents que les Archives de l'État prennent en dépôt peuvent contenir des informations à caractère personnel et, pour autant qu'elles concernent des personnes qui sont encore en vie, leur traitement peut tomber sous l'application de la loi relative à la protection de la vie privée (ci-après LVP). Cette éventualité augmente évidemment au fur et à mesure que le délai d'attente pour l'accès aux documents diminue et que notre espérance de vie progresse. Par ailleurs, certaines figures historiques survivent dans les esprits et les historiens se font un plaisir de revenir, à la grande joie de beaucoup, sur ce qui serait considéré comme une atteinte ignoble à la vie privée à l'égard de personnes vivantes. Dans certains cas, cela peut être à ce point humiliant pour les proches ou les descendants que cela peut être considéré à leur égard comme une violation de la LVP. [...] la LVP demeure applicable à des données à caractère personnel concernant des personnes vivantes et à des données à caractère personnel concernant des personnes décédées, dans la mesure où leur traitement menace gravement la vie privée de proches. »[5]

Dix ans plus tard, la Commission a publié deux brochures, la première relative à l'application de la loi vie privée dans le cadre de la recherche historique, la deuxième portant sur l'application de la loi vie privée au domaine de la recherche biomédicale. À cette occasion, la Commission de la protection de la vie privée a, selon ses termes, « adopté des décisions de principe » concernant notamment les données ayant trait aux personnes vivantes et aux personnes décédées. « Dans les brochures, le concept de "donnée à caractère personnel" est défini comme étant toute donnée apportant des informations sur une personne vivante. On ajoute que les données relatives à des personnes décédées ne sont en principe pas protégées par la législation vie privée. Cela n'empêche pas qu'une personne décédée et ses données puissent bénéficier d'une protection offerte par une autre réglementation [...]. Cela n'empêche

1. J. Herveg, « La protection des données du patient après son décès : une persistance du droit au respect de la vie privée ? », *in Défis du droit à la protection à la vie privée*, coll. Cahiers du CRID, vol. 31, 2008, pp. 209 à 242 ; C. Decoster, « De verwerking van medische persoonsgegevens », *A. Hosp.*, 1994, p. 27.
2. À titre d'exemple, le Tribunal civil de Bruxelles a jugé, sur la base d'un raisonnement portant sur l'analyse des droits des personnes concernées tels que libellés dans la loi vie privée, que la protection des données perdurait même après le décès de la personne. Dans le dossier soumis au tribunal, des ayants droit d'un patient décédé souhaitaient avoir communication du dossier médical de ce patient (Civ. Bruxelles, 25 mars 2005, *J.L.M.B.*, 2006, p. 1197).
3. C.P.V.P., avis d'initiative du 15 juin 2000 relatif au droit d'accès des héritiers au dossier médical du défunt, n° 19/2000.
4. C.P.V.P., avis n° 49/2001 du 10 décembre 2001 relatif aux archives de l'État.
5. Même si la Commission de la protection de la vie privée ne le dit pas, il s'agit de menaces à l'égard de proches encore vivants.

pas non plus que des données à caractère personnel d'une personne décédée puissent également contenir des informations personnelles d'autres personnes (toujours vivantes), comme des membres de la famille ou des proches. La LVP s'appliquera à ces données dans la mesure où elles peuvent être considérées comme des données à caractère personnel dans le chef de la famille ou des proches encore en vie »[1].

Il semble donc clair aujourd'hui aux yeux de la Commission que des données se rapportant à des personnes décédées ne peuvent pas bénéficier de la protection accordée aux données à caractère personnel, à moins qu'elles ne concernent également des personnes encore en vie. Il existe effectivement des cas où les données ne sont pas purement individuelles et peuvent donc concerner d'autres personnes[2]. Les données génétiques d'une personne morte peuvent ainsi être rattachées à ses descendants (affections héréditaires) et sont par conséquent à considérer comme des données à caractère personnel dans le chef de ces derniers. Il en est de même des liens de filiation.

Personne identifiée ou identifiable

Si la loi ne définit pas la « personne concernée », elle donne cependant les clés de compréhension de cette notion. Ainsi, la « personne concernée » peut être définie comme étant la personne physique identifiée ou identifiable à laquelle les données à caractère personnel se rapportent.

La loi précise qu'« est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[3].

Il est important de relever que, par identification, il ne faut pas nécessairement entendre la détermination de l'identité civile d'un individu, mais bien plutôt la possibilité de **distinguer** une personne parmi d'autres. En ce sens le Groupe de l'article 29 a indiqué : « D'une manière générale, on peut considérer une personne physique comme "identifiée" lorsque, au sein d'un groupe de personnes, elle se "distingue" de tous les autres membres de ce groupe »[4].

Plutôt qu'opter pour une évaluation *in concreto* du caractère identifiable de la personne concernée, c'est-à-dire en tenant compte des moyens à disposition du responsable du traitement des données, l'Exposé des motifs de la loi signale qu'il

1. C.P.V.P., *Rapport annuel 2011*, point 7.7. Vade-mecum relatif à la recherche biomédicale, http://www.privacycommission.be/sites/privacycommission/files/documents/vade-mecum-recherche-biomedicale_0.pdf.
2. C.P.V.P., avis n° 25/2011 du 19 octobre 2011 relatif au projet d'arrêté royal fixant les normes auxquelles une fonction « coordination locale des donneurs » doit répondre pour être agréée et le rester.
3. Article 1er, § 1er, de la loi du 8 décembre 1992.
4. Groupe de l'article 29, *WP* 136, préc., p. 13.

convient d'évaluer *in abstracto* le caractère identifiable. Les auteurs de la loi se sont appuyés sur le considérant n° 26 de la directive 95/46[1] pour opérer ce choix. Pour déterminer si une personne est identifiable, il faut prendre en compte « l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre par le responsable du traitement *ou par toute autre personne*, pour identifier les sujets de données »[2].

En conséquence, si celui qui utilise les données n'a pas lui-même la possibilité d'identifier les individus correspondant aux données mais qu'il se trouve quelqu'un raisonnablement apte à le faire, les données doivent tout de même être considérées comme étant « à caractère personnel ». Cela induit que la loi s'appliquera au traitement de telles données. Cela rend la définition de la donnée à caractère personnel extrêmement large étant donné que, dès l'instant où quelqu'un sera en mesure d'identifier la personne concernée par une donnée, il s'agira d'une donnée à caractère personnel.

Ce raisonnement *in abstracto* pour évaluer si une personne est identifiable ou non a été appliqué par le Groupe consultatif de l'article 29 aux *adresses IP*. Ces données identifiant (distinguant) l'ordinateur transmises lors de sessions Internet, ont été considérées comme des données à caractère personnel par ce Groupe à l'occasion de l'avis qu'il a émis concernant les moteurs de recherche[3]. Ainsi, aux termes de cet avis, « [l]'historique des recherches d'une personne constitue des données à caractère personnel si la personne concernée est identifiable. Or, bien que dans la plupart des cas, les adresses IP ne soient pas directement identifiables par les moteurs de recherche, un tiers peut parvenir à identifier la personne en question. Les fournisseurs d'accès à Internet disposent en effet des données relatives à l'adresse IP. Les autorités répressives et les services nationaux de sécurité peuvent obtenir l'accès à ces données et, dans certains États membres, des personnes privées ont également obtenu cet accès dans le cadre de procédures judiciaires civiles. Ainsi, dans la plupart des cas – y compris dans ceux impliquant une adresse IP dynamique – les données nécessaires existent pour identifier le ou les utilisateur(s) de l'adresse IP »[4].

Identifiable par des moyens raisonnables

Pour considérer des personnes comme identifiables, il faut toutefois, et c'est le critère essentiel, que les moyens d'identification soient « susceptibles d'être raisonnable-

1. Considérant n° 26 de la directive 95/46 : « considérant que les principes de la protection doivent s'appliquer à toute information concernant une personne identifiée ou identifiable ; que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne ; que les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable ; [...] »
2. Projet de loi transposant la directive (CE) 95/46 du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Exposé des motifs, *Doc. parl.*, Chambre, 1997-1998, n° 1566/1.
3. Groupe de l'article 29, avis 1/2008 du 4 avril 2008 sur les aspects de la protection des données liés aux moteurs de recherche, *WP* 148.
4. *Ibid.*, p. 9.

ment mis en œuvre ». La législation invite donc à ne prendre en compte que les moyens raisonnables. *Il ne faut pas, notamment, que les moyens susceptibles d'être mis en œuvre induisent une violation de la loi pour conduire à l'identification de la personne concernée.*

Ainsi, si l'on se trouve en présence de données médicales se rapportant aux patients d'un médecin et que ces données sont communiquées sous forme codée à un chercheur, on observe que la personne capable d'identifier les personnes visées par ces données codées est un médecin tenu, en tant que tel, par l'obligation de secret médical. Dans ce cas, le responsable du traitement (le chercheur) ou une autre personne ne pourraient pas raisonnablement obtenir l'identification auprès du médecin. En conséquence, ces données codées ne doivent pas être considérées comme étant « à caractère personnel »[1]. De telles données pourraient cependant être considérées à caractère personnel si le chercheur procède à un traitement qui permet l'identification de la personne concernée. L'on voit donc qu'il faut, pour chaque traitement, procéder à une nouvelle analyse du caractère personnel, ou non, des données ainsi que nous le verrons ci-après pour les *adresses IP.*

Concernant les ***adresses IP***, outre ce qui a été mentionné ci-dessus, on relèvera que le Groupe de l'article 29 lie, dans une certaine mesure, le caractère identifiable des adresses IP au contexte dans lequel ces données sont traitées. C'est ainsi en prenant en considération les moyens raisonnables à disposition de certains acteurs mus par un objectif d'identification, que le Groupe de travail a spécifié que les adresses IP constituaient des données à caractère personnel dans ces circonstances. Dans son avis sur la notion de donnée à caractère personnel, le Groupe de travail a ainsi affirmé, en visant spécifiquement les sociétés titulaires de droits de propriété intellectuelle ratissant Internet en vue de collecter des données permettant de remonter jusqu'aux personnes violant ces droits : « Il apparaît notamment que *lorsque le traitement d'adresses IP est effectué pour identifier les utilisateurs de l'ordinateur* (par exemple, par des titulaires de droits d'auteur afin de poursuivre ces utilisateurs d'ordinateurs pour violation de droits de la propriété intellectuelle), le responsable du traitement part du principe que les "moyens susceptibles d'être raisonnablement mis en œuvre" pour identifier les personnes seront disponibles, par exemple par l'intermédiaire des tribunaux saisis (sinon la collecte d'informations serait inutile), de sorte qu'il convient de considérer ces informations comme des données à caractère personnel »[2]. Dans le même sens, visant cette fois les fournisseurs d'accès, les gestionnaires de réseaux et les fournisseurs de services Internet : « les fournisseurs d'accès Internet et les gestionnaires des réseaux locaux peuvent, en utilisant des moyens raisonnables, identifier les utilisateurs Internet auxquels ils ont attribué des

1. Voy., dans le même sens, l'avis 4/2007 du Groupe de l'article 29 sur le concept de donnée à caractère personnel, *WP* 136, adopté le 20 juin 2007. L'exemple 13, p. 17, reprend précisément le cas de données médicales codées transmises à une société pharmaceutiques, seuls les médecins tenus au secret professionnel connaissant le nom des patients. Le Groupe de l'article 29 conclut que les données codées ne sont pas, dans ce cas, des données à caractère personnel.
2. Groupe de l'article 29, *WP* 136, préc., p. 18 (nous soulignons).

adresses IP, du fait qu'ils enregistrent systématiquement dans un fichier les date, heure, durée et adresse dynamique IP donnée à l'utilisateur Internet. Il en va de même pour les fournisseurs de services internet qui conservent un fichier-registre sur le serveur HTTP. Dans ces cas, on peut parler, sans l'ombre d'un doute, de données à caractère personnel au sens de l'article 2, point a), de la directive »[12].

La Cour de justice de l'Union européenne a considéré de la même manière, dans les affaires *Scarlet*[3] et *Bonnier*[4], que constituent des données à caractère personnel les adresses IP des utilisateurs à l'origine de l'envoi de contenus illicites sur le réseau, dans la mesure où leur collecte et traitement visent à identifier précisément ces utilisateurs.

Données codées

L'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel donne une définition de ce qu'il faut entendre par « données à caractère personnel codées » : « les données à caractère personnel qui ne peuvent être mises en relation avec une personne identifiée ou identifiable que par l'intermédiaire d'un code »[5].

Les données codées ne font en fait pas nécessairement partie de la catégorie des données à caractère personnel. Cela dépend du sort réservé à la clé du code qui permet de faire le lien entre une donnée codée et la personne à laquelle cette donnée se rapporte. En effet, si la clé du code a été conservée et qu'il se trouve quelqu'un – le responsable du traitement ou un tiers – qui détient cette clé et peut raisonnablement réidentifier les personnes concernées, les données codées seront considérées comme étant à caractère personnel. Tandis que, si la clé du code n'a pas été conservée et que plus personne n'est en mesure de faire le lien entre les données codées et les personnes concernées, on se trouve en présence de données qui ne sont pas à caractère personnel mais anonymes (donc non couvertes par la loi de 1992).

---

1. Groupe de l'article 29, 21 novembre 2000, « Le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne », *WP* 37 (nous soulignons).
2. À ce sujet, voy. J.-Ph. Moiny, « Are Internet protocol addresses personal data ? The fight against online copyright infringement », *C.L.S.R.*, 27, 2011, pp. 348 à 361.
3. C.J.U.E., 24 novembre 2011 (Scarlet Extended v. SABAM), aff. C-70/10, point 51.
4. C.J.U.E., 19 avril 2012 (Bonnier Audio AB c. Perfect Communication Sweden AB), aff. 461/10, points 51 et 52 : « [...] il convient, d'abord, de rappeler que, dans l'affaire au principal, Bonnier Audio e.a. souhaitent la communication, aux fins de son identification, du nom et de l'adresse d'un abonné à Internet ou d'un utilisateur d'internet faisant usage de l'adresse IP à partir de laquelle il est présumé que des fichiers contenant des œuvres protégées ont été illicitement échangés. Il y a lieu de constater que la communication souhaitée par Bonnier Audio e.a. constitue un traitement de données à caractère personnel au sens de l'article 2, premier alinéa, de la directive 2002/58, lu en combinaison avec l'article 2, sous b), de la directive 95/46. »
5. Article 1er, 3°, de l'arrêté royal du 13 février 2001.

Ainsi qu'évoqué au paragraphe précédent, rappelons que des données médicales codées ne sont pas des données à caractère personnel dès lors que seul un médecin tenu au secret professionnel détient la clé du code et que le chercheur ne procède pas à un traitement permettant l'identification de la personne concernée.

Données anonymes

Aux termes de l'article 1er, 5°, de l'arrêté royal du 13 février 2001 exécutant la loi vie privée, les données anonymes sont à entendre comme « les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont donc pas des données à caractère personnel ».

Le considérant n° 26 de la directive 95/46 précise, quant à lui, que « les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable ».

La Commission de la protection de la vie privée a précisé qu'il ne suffit pas de dépersonnaliser des données à caractère personnel pour pouvoir les considérer comme des données anonymes. En effet, « la suppression de données d'identification ne permet pas toujours d'empêcher que les personnes concernées soient à nouveau identifiées ou pour le dire autrement, n'élimine pas complètement le risque que leur identité soit néanmoins découverte. Dès lors, tant que subsiste une possibilité théorique de réidentification, il n'est pas permis de parler de données anonymes »[1]. Il était d'ailleurs indiqué dans l'Exposé des motifs de la loi du 11 décembre 1998 modifiant la loi de 1992 pour la mettre en conformité avec la directive 95/46 : « Une information relative à une personne est donc considérée comme une donnée à caractère personnel tant que quelqu'un est encore en mesure, par quelque moyen qui puisse raisonnablement être mis en œuvre, de déterminer à quel individu se rapporte cette information. [...] Lorsque les informations relatives à des personnes physiques sont rendues anonymes, elles ne perdent donc leur caractère de données à caractère personnel que si le caractère anonyme est absolu et que plus aucun moyen raisonnablement susceptible d'être mis en œuvre ne permet de revenir en arrière pour briser l'anonymat ».

La question de l'anonymisation des données doit par ailleurs impérativement être envisagée dans un contexte technique en perpétuelle évolution. Ce qui dépasse à un moment donné les limites du raisonnable pour procéder à la mise en relation des données avec les personnes auxquelles elles se rapportent est susceptible de devenir à la portée de certains, voire de tous, dans un délai plus ou moins rapproché au vu des développements des capacités techniques. Le caractère anonyme d'une

1. C.P.V.P., avis n° 4/2006 du 8 février 2006 relatif à l'avant-projet de loi transposant la directive 2003/98 du Parlement européen et du Conseil concernant la réutilisation des informations du secteur public.

donnée doit donc faire l'objet, de manière régulière, d'une réévaluation afin de s'assurer du maintien de cet anonymat.

Enfin, des statistiques pourtant anonymes peuvent, si elles présentent un niveau trop fin d'agrégation, soulever des difficultés au regard des principes issus de la législation de protection des données à caractère personnel[1]. En effet, le caractère anonyme des informations statistiques peut être mis à mal par les techniques (pratiquées par les entreprises de marketing) consistant à identifier un petit groupe de population (correspondant à un îlot, niveau d'agrégation le plus fin) présentant des caractéristiques communes. Par des recoupements avec divers fichiers (données du recensement de la population, de l'annuaire téléphonique et du cadastre, par exemple), on parvient à l'identification des individus avec un très haut taux de probabilité. Des seuils minimaux d'agrégation sont donc à fixer pour que la diffusion de données statistiques anonymes ne heurte pas les droits garantis par la législation de protection des données[2].

2.1.3. Catégories de données : données normales et données sensibles

La loi vie privée distingue certaines catégories de données à caractère personnel dont le traitement suit des règles de protection différentes.

La première catégorie de données est celle rassemblant les données que l'on peut qualifier de normales dans la mesure où ces données ne sont pas susceptibles *in se* de porter atteinte aux libertés fondamentales ou à la vie privée des personnes concernées. Il s'agit d'une catégorie « par défaut » dès lors que s'y retrouvent toutes les données qui ne sont pas visées par les articles 6, 7 et 8 de la LVP, articles consacrés au régime plus protecteur des données de la deuxième catégorie, les données « sensibles ». Une protection accrue est accordée aux données dites sensibles qui rassemblent trois sous-catégories de données : les données relatives à la santé (visées à l'art. 7 LVP), celles se rapportant aux condamnations pénales et administratives ainsi qu'aux suspicions (visées à l'art. 8[3]) et, enfin, les données sensibles au sens strict (visées par l'art. 6 de la loi) : les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale et les données relatives à la vie sexuelle.

C'est principalement le risque de discriminations illégitimes ou arbitraires qui est lié à ces données qui justifie le traitement différencié qui leur est accordé. De telles données présentent, en outre, un risque d'affecter la sphère la plus intime des sujets de

1. M. Van Overstraeten et S. Depré, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, p. 675.
2. Voy. l'avis de la Commission (française) nationale de l'informatique et des libertés, *10e Rapport d'activités*, Paris, La Documentation française, 1989, pp. 11 et s.
3. Plus précisément, l'article 8 LVP concerne « [l]e traitement de données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté ».

données, ainsi qu'un risque sérieux de dommage, en cas d'abus, pour la personne concernée[1].

Données sensibles par nature/en fonction du contexte

La question des données sensibles suscite l'éternel débat entre tenants de l'hypothèse où c'est le contexte d'utilisation, la finalité du traitement envisagé qui rend les données sensibles et ceux qui estiment indispensable d'établir une liste de données sensibles par nature. Le recours à une telle liste déclenche automatiquement l'application d'un régime de protection renforcé lié au risque d'affecter la sphère la plus intime des individus ou d'engendrer des discriminations illégitimes ou arbitraires sur la base des données visées. Une telle liste permet donc d'évacuer toute interrogation contextuelle.

La définition des données sensibles présentée sous forme de liste à l'article 6 de la loi n'est pas sans susciter un certain malaise. La formulation est effectivement extrêmement large du fait que sont couvertes par le régime particulier les « données à caractère personnel *qui révèlent* l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, [...] »[2]. Cela signifie, en effet, que tombent dans cette catégorie, par exemple, les noms patronymiques qui révèlent indubitablement l'origine raciale, de même que toute photo d'une personne ; l'achat d'un ouvrage sur le Coran sur un site Web peut, quant à lui, révéler les convictions religieuses, etc. Or il est inconcevable de traiter systématiquement les noms, les photographies et certains achats comme des données sensibles bénéficiant d'un régime de protection particulièrement sévère. Ce ne sera que quand c'est justement l'élément sensible de la donnée qui est retenu par le responsable du traitement (sélection des personnes d'origine russe ou japonaise, sur la base de leurs noms ; ou sélection des personnes de type maghrébin, tutsi, rom ou aborigène sur la base de leurs photos) que le régime protecteur, principalement lié au risque élevé de discrimination à partir des données traitées, se justifie[3]. C'est pour contrer un risque de discrimination de ce type lors des embauches que se développe la pratique de sélectionner les candidats à un poste professionnel sur la base de curriculum vitae sans nom apparent.

D'une part, il est louable de retenir les données « qui révèlent » des caractéristiques sensibles des personnes. Cela permet en effet de considérer comme sensibles des cas dans lesquels n'apparaît aucune donnée *a priori* sensible. Ainsi, les recherches sur Google de sites sur le pèlerinage de Saint-Jacques de Compostelle pratiquées

1. Voy. article 13, § 1er, de la Résolution de Madrid, *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the Processing of Personal Data*, disponible à l'adresse http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf.
2. C'est nous qui soulignons.
3. Voy., dans le même sens, TH. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 386, spéc. la note 106.

par un internaute, son achat de livres religieux, sa lecture d'une encyclique pontificale, etc., pourraient être traités comme révélant une opinion religieuse.

D'autre part, retenir justement tout ce qui révèle une caractéristique sensible en arrive, ainsi qu'on l'a dit, à faire entrer dans cette catégorie de données énormément de données qui dans bien des cas ne sont pas traitées pour l'aspect sensible qu'elles véhiculent. Cela est excessif et risque d'ôter son sens à la notion de données sensibles au niveau de l'application concrète.

La Commission de la protection de la vie privée a adopté plusieurs avis qui reflètent cette difficulté issue des termes de la loi du 8 décembre 1992 (termes fidèles, il faut le dire, à la formule de la directive 95/46, elle-même dans la ligne de la Convention 108 du Conseil de l'Europe...). Lors des auditions au Sénat précédant l'adoption de la législation en matière de vidéosurveillance, le président de la Commission l'a affirmé : « toute information n'est pas forcément sensible en elle-même, ces caractéristiques pouvant résulter du contexte et des finalités pour lesquelles les données sont traitées. Ainsi, la couleur de la peau des personnes filmées, qu'elle soit blanche ou noire, ne peut être considérée comme sensible en elle-même, mais elle le serait si par exemple l'objectif de l'enregistrement d'images était d'identifier et de classer les personnes filmées selon leur couleur de peau »[1]. À plusieurs reprises, la Commission avait déjà considéré que, si l'on pouvait déduire une information relative à l'état de santé d'une personne sur la base du port de lunettes ou d'un bandage autour du bras de la personne, ces images ne devaient pas être assimilées à des données médicales à caractère personnel dans les cas où ces caractéristiques ne sont pas utilisées pour en déduire systématiquement une information sur l'état de santé des personnes identifiées[2].

Plus récemment, le comité sectoriel de l'Autorité fédérale instauré au sein de la Commission de la protection de la vie privée a réitéré cette position en faveur d'une prise en compte du contexte, de la finalité d'utilisation des données en cause avant de leur appliquer le régime des données sensibles. Le comité sectoriel était saisi d'une demande portant sur la communication au Service des Pensions du Secteur public de l'information relative au statut de grand invalide de guerre accordé à certaines personnes concernées. Le Comité a estimé que, « [s]i l'on interprète l'article 7, § 1er de la LVP de façon stricte, cette information pourrait le cas échéant être qualifiée de donnée à caractère personnel relative à la santé. Le comité estime toutefois qu'une telle donnée n'est pas en soi nécessairement sensible, mais que son caractère sensible résulte éventuellement du contexte et des finalités pour lesquelles les données

1. Audition de MM. M. Parisse et W. De Beuckelaer, président et vice-président de la Commission de la protection de la vie privée, « Surveillance par caméra », Rapport, Sénat, 2005-2006, *Document législatif*, n° 3-1413/1.
2. C.P.V.P., avis n° 14/95 du 7 juin 1995 sur l'applicabilité de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel à l'enregistrement d'images et ses conséquences ; C.P.V.P., Recommandation n° 01/98 du 14 décembre 1998 en matière de Système informatisé de réservation ; C.P.V.P., avis n°17/99 du 10 mai 1999 relatif au projet d'arrêté royal concernant l'installation et le fonctionnement de caméras de surveillance dans les stades de football.

sont traitées. Étant donné que le présent traitement du demandeur s'inscrit dans un contexte purement administratif et n'a en outre pour but que d'octroyer un avantage fiscal aux personnes concernées, le comité estime [...] qu'il ne s'agit en l'occurrence pas d'une donnée à caractère personnel relative à la santé et donc qu'aucun régime de protection plus strict ne s'applique »[1].

Enfin, dernièrement, la Commission a maintenu son approche contextualisée dans un avis portant sur les tests d'alcoolémie ou de détection de drogues[2]. Elle a ainsi affirmé : « La question de savoir si et dans quelles circonstances concrètes le résultat d'un test individuel d'alcoolémie ou de détection de drogues (qui ne constitue pas un traitement médical) doit être considéré comme une donnée relative à la santé ne doit *a priori* pas être examinée ici. Certaines données sont par nature des données relatives à la santé, d'autres permettent seulement potentiellement de déduire des informations relatives à l'état de santé physique ou psychique antérieur, actuel ou futur de la personne concernée. Dans les cas où le traitement des résultats des tests constitue un traitement de données relatives à la santé, la Commission estime que cela peut et doit se faire dans le cadre de l'article 7 de la LVP. Il est clair que l'employeur qui fait subir à un membre du personnel, pendant une certaine période, plusieurs tests d'alcoolémie et/ou de détection de drogues dans le but, après un certain temps, de confirmer (ou de voir réfutés) ses soupçons que la personne concernée a un problème d'alcool ou de drogue, procède à un traitement de données relatives à la santé au sens de l'article 7 de la LVP. *L'élément déterminant n'est* pas le nombre de tests subis mais *la manière dont les résultats sont utilisés* »[3].

Le juge devra donc analyser la question de manière contextuelle.

2.2. La notion de « Traitement »

2.2.1. Définition de la loi vie privée

Par traitement, l'on doit entendre « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposi-

1. Comité sectoriel pour l'Autorité fédérale, Délibération AF n° 10/2008 du 20 novembre 2008 concernant une demande d'autorisation formulée par l'Agence « Vlaamse Belastingdienst » (VLABEL) (Service flamand des Impôts) en vue du traitement de données à caractère personnel enregistrées dans des banques de données de l'Administration générale de la Documentation patrimoniale et du Service des Pensions du secteur public.
2. C.P.V.P., avis n° 36/2012 du 12 décembre 2012 concernant un avant-projet de loi portant certaines dispositions du statut administratif du personnel opérationnel des zones de secours et le livre 15 d'un avant-projet d'arrêté royal relatif au statut administratif du personnel opérationnel des zones de secours, portant sur l'exécution d'un test d'alcoolémie ou de détection de drogues (CO-A-2012-043).
3. *Ibid.*, nous soulignons.

tion, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel »[1].

Le traitement est donc un ensemble d'opérations extrêmement variées que l'on applique à des données à caractère personnel. En fait, tout ce qui peut être fait avec des données à caractère personnel, tout type d'actions ou d'utilisations des données entre dans la définition de « traitement ».

Son intention étant de protéger les individus dès l'instant où l'on collecte ou l'on enregistre les informations se rapportant à eux, le législateur a veillé à faire intervenir la notion de traitement dès l'instant où une opération, même unique, est appliquée aux données.

2.2.2. Le critère de définition d'un traitement

C'est la finalité attachée à un ensemble d'opérations appliquées à des données à caractère personnel qui donnera à ces différentes opérations leur cohérence et permettra de conclure que l'ensemble forme un traitement de données. La finalité est l'élément unificateur du traitement[2]. Ce critère de définition « consacre la théorie de la finalité générique »[3]. La finalité de gestion du personnel, par exemple, implique une grande variété d'applications qui peuvent être envisagées comme formant un tout, un seul traitement visant à la gestion du personnel[4].

Un traitement peut poursuivre plusieurs finalités mais celles-ci doivent être compatibles entre elles pour être jugées comme attachées au même traitement. Si une finali-

---

1. Article 1er, § 2 ; voy. également, sur cette notion, Cass., 16 mai 1997, *J.T.*, 1997, p. 779 ; Anvers, 27 septembre 1995, *A.J.T.*, 1995-1996, note J. DUMORTIER et TH. LÉONARD, « La protection des données à caractère personnel et l'entreprise », *in Guide juridique de l'entreprise*, 2e éd., titre XI, liv. 112, Diegem, Kluwer, 1996, p. 15, n° 130 ; M.-H. BOULANGER, C. DE TERWANGNE et TH. LÉONARD, « La protection de la vie privée à l'égard des traitements de données à caractère personnel. La loi du 8 décembre 1992 », *J.T.*, 1993, p. 372 ; TH. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, p. 379 ; M. VAN OVERSTRAETEN et S. DEPRÉ, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, pp. 678 et s. ; en France, voy. notamment : Cass. (ch. crim.), 3 novembre 1987, *D.*, 1988, J., pp. 17 et s., note H. Maist ; Trib. gr. inst. Créteil, 10 juillet 1987, *D.*, 1988, J., pp. 319 et s., note J. Frayssinet ; J. FRAYSSINET, « La Cour de Cassation et la loi informatique, fichiers et libertés ou comment amputer une loi tout en raffermissant son application », *J.C.P.*, 1988, I, n° 3223 ; IDEM, « Contre l'excessive distinction entre fichier et dossier – Le pas en avant du tribunal correctionnel de Paris », *Expertises*, 1990, pp. 16 et s.
2. TH. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 379. Voy. également TH. LÉONARD, « La protection des données à caractère personnel et l'entreprise », *Guide juridique de l'entreprise*, *op. cit.*
3. P. DE HERT et D. PISSOORT, *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2004, p. 73.
4. On ne suit donc pas B. Docquir qui a perdu de vue ce critère lorsqu'il affirme que, « [...] en pratique, les données collectées en vue d'un traitement déterminé feront toujours l'objet de nombreux traitements ultérieurs. Elles pourront, par exemple, être archivées, intégrées à une autre base de données, vendues ou louées à des tiers, vérifiées et croisées avec d'autres données, enrichies, voire simplement effacées ou détruites. Chacune de ces opérations constitue un traitement nouveau aux yeux de la loi et doit donc être compatible avec les finalités du traitement initial. » (B. DOCQUIR, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, p. 125). Si toutes les opérations évoquées par cet auteur sont effectuées en vue de réaliser une même finalité, il s'agit en fait d'un seul traitement, puisque, par définition, ce terme recouvre un ensemble varié d'opérations appliquées à des données.

té n'est pas compatible avec la première, elle se rattache à un traitement différent du premier[1].

2.2.3. Tout type d'opérations

Ainsi qu'on l'a dit, la notion de traitement retenue par le texte légal est à ce point large que toute opération, depuis la collecte jusqu'à la destruction, est constitutive de traitement. Le fait de collecter ou de consulter des données à caractère personnel est déjà considéré comme un traitement de données à caractère personnel. Le simple visionnage d'images de personnes captées par une caméra de surveillance, que ces images soient ou non enregistrées, correspond à un traitement de données au sens de la loi.

Il en va de même lorsqu'un logiciel de traitement de texte est utilisé pour enregistrer des données à caractère personnel. La Cour d'appel de Mons a ainsi considéré que « le rapport d'un détective privé constitue en effet un traitement de données à caractère personnel au sens de la loi du 8 décembre 1992 lorsque, comme en l'espèce, il contient [des données à caractère personnel], à savoir toute information se rapportant à une personne physique identifiée ou identifiable, lorsque ces données ont subi un "traitement automatisé", à savoir tout traitement dans lequel l(es) technologie(s) de l'information (et de la communication) intervien(nent), tel que le traitement de texte utilisé en informatique »[2].

Dans un arrêt du 19 novembre 2009, la Cour d'appel de Liège a considéré, pour sa part, que le fait, pour un gestionnaire de site Internet, d'enregistrer et de conserver des données pour lui permettre d'envoyer des courriels non sollicités constitue un traitement de données à caractère personnel[3].

Dans un autre contexte, une base de données commercialisée, concernant des informations commerciales relatives à des sociétés (mais contenant des noms d'individus identifiés) a été considérée, en tant que banque de données automatisée pouvant être consultée en ligne par les clients, comme incluse dans la notion de traitement[4].

Il a aussi été affirmé que la consultation et l'utilisation de données du répertoire d'immatriculation des véhicules (D.I.V.) étaient constitutives d'un traitement de données. De même, le transfert de données de la D.I.V. à des entreprises privées par les services communaux, via un détour par la commune (le bourgmestre, la police ou le receveur communal), constitue un traitement de données couvert par la loi[5].

---

1. Th. Léonard et Y. Poullet, *op. cit.*, p. 379 ; P. De Hert et D. Pissoort, *op. cit.*, p. 74.
2. Mons (14e ch.), 2 mars 2010, *R.D.T.I.*, n° 41/2010, p. 83, note F. Dumortier.
3. Liège (7e ch.), 19 novembre 2009, *D.A. O.R.*, 2010/96, p. 453.
4. Comm. Courtrai (1re ch.) 19 juin 2003, *T.G.R.-T.W.V.R.*, 2007, liv. 2, p. 97.
5. J.P. Mol, 11 janvier 2005, *R.W.*, 2007-2008, liv. 11, pp. 448 et 449.

2.2.4. La consultation comme opération unique

Une question particulière concerne la consultation proprement dite. Ainsi que déjà signalé, chacune des opérations énumérées dans la définition légale du traitement, même prise isolément, met en présence d'un traitement. En conséquence, la simple consultation de données à caractère personnel peut impliquer l'existence d'un traitement.

Or appliquer cela à la lettre conduirait à une multiplication exponentielle des traitements visés par la loi[1]. En effet, toute personne ne faisant rien d'autre que consulter un site Internet dans lequel apparaissent des données à caractère personnel (nom des membres d'un cabinet d'avocats, liste de résultats sportifs, nom de l'auteur d'un billet posté sur le Net...) serait en train d'effectuer un traitement de données. Cette personne serait dès lors soumise aux obligations contenues dans la loi (faire la déclaration du traitement auprès de la Commission de la vie privée, informer les personnes concernées qu'elle a effectué un traitement impliquant des données à propos d'elles, leur accorder un droit d'accès aux données traitées...). Il est clair que de telles implications sont pour le moins problématiques, particulièrement lorsque la consultation n'est suivie d'aucune matérialisation (enregistrement ou impression des données, par exemple). Il n'est évidemment pas envisageable de donner accès à des données ayant fait l'objet d'un traitement éphémère n'ayant laissé aucune trace si ce n'est dans la mémoire de celui qui a consulté les données. Par ailleurs, il semblerait totalement absurde de devoir informer les personnes à propos de qui des données sont diffusées publiquement (sur un site Internet, mais aussi dans l'annuaire téléphonique ou dans le dictionnaire des noms propres !) que vous avez consulté ces informations. Il est important de percevoir que la consultation de données est une opération qui ne doit pas être envisagée isolément, mais qui se situe au terme d'une chaîne d'opérations visant à rendre des données à caractère personnel accessibles. La personne qui visualise les données, qui les consulte est le dernier maillon de la chaîne. C'est l'ensemble de la chaîne qui forme un traitement aux yeux de la loi. Le responsable de ce traitement sera la personne qui décide de rendre les données accessibles et de les diffuser via Internet, l'annuaire, le dictionnaire ou autre. Le lecteur n'initie pas un nouveau traitement tant qu'il ne fait que prendre connaissance des données. Si, par contre, il utilise les données pour une finalité différente de celle ayant présidé à la diffusion, il démarrera un nouveau traitement, différent du premier, et deviendra à ce moment responsable de ce nouveau traitement. Ce sera le cas, par exemple, s'il utilise le numéro de téléphone consulté pour faire du démarchage commercial à l'égard de l'abonné. La mise à disposition des numéros de téléphone dans l'annuaire poursuit la finalité de permettre la mise en communication de deux personnes, mais non l'utilisation des informations diffusées à des fins de marketing direct.

---

1. M.-H. Boulanger et C. de Terwangne, « Internet et le respect de la vie privée », *in Internet face au droit*, Cahiers du CRID, n° 12, Namur, Story-Scientia, 1997, pp. 198 et 199 ; M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau et Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, pp. 125 et 126.

2.3. La notion de « Fichier »

Il est également utile de rappeler que la notion de traitement ne s'applique pas uniquement lors d'opérations à l'aide de procédés automatisés mais également à des traitements manuels. En effet, la loi vie privée « s'applique à tout traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier »[1].

Par fichier, il faut entendre « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »[2].

En clair, pour que la loi s'applique également à un traitement effectué par des moyens non automatisés; « il faut des données ordonnées et que celles-ci soient accessibles en fonction de critères déterminés. À cet égard, l'ordre et la méthode conduisent inévitablement à l'application de la loi »[3]. Un classement sur la base des noms des personnes, par ordre alphabétique, constitue un fichier au sens de la loi vie privée. Il en est de même des classements selon un critère géographique, chronologique ou sur la base de résultats, etc.

La classification des données distingue donc le fichier du dossier qui, lui, n'est pas couvert par la loi. Le critère de distinction entre fichier et dossier se situe dans le degré d'accessibilité des données contenues. Ces données doivent être accessibles selon des critères déterminés pour que l'ensemble soit considéré comme fichier. Un rassemblement de données non structurées et sur papier correspond à un dossier[4].

La consultation de documents papier isolés ou l'envoi par courrier ordinaire de photocopies de documents papier qui ne sont pas extraits d'un « ensemble structuré de données à caractère personnel accessibles selon des critères déterminés » ne correspondent pas à un traitement de données conservées dans un fichier et peuvent se faire sans tenir compte des principes régissant la protection des données à caractère personnel.

---

1. Article 3, § 1er.
2. Article 1er, § 3.
3. C. DE TERWANGNE, J. HERVEG et J. -M. VAN GYSEGHEM, *Le divorce et les technologies de l'information et de la communication : introduction à la protection des données dans la preuve des causes de divorce*, Kluwer, 2005, p. 12
4. La différence entre fichier et dossier a fait couler beaucoup d'encre et a fait l'objet, en Belgique, d'un arrêt en cassation : Cass., 16 mai 1997, *J.T.*, 1997, p. 779 ; Anvers, 27 septembre 1995, *A.J.T.*, 1995-1996, note J. Dumortier ; TH. LÉONARD, « La protection des données à caractère personnel et l'entreprise », *in Guide juridique de l'entreprise*, 2e éd., titre XI, liv. 112, Diegem, Kluwer, 1996, p. 15, n° 130 ; en France, voy. notamment : Cass. (ch. crim.), 3 novembre 1987, *D.*, 1988, J, pp. 17 et s., note H. Maisl ; Trib. gr. inst. Créteil, 10 juillet 1987, *D.*, 1988, J., pp. 319 et s., note J. Frayssinet ; J. FRAYSSINET, « La Cour de Cassation et la loi informatique, fichiers et libertés ou comment amputer une loi tout en raffermissant son application », *J.C.P.*, 1988, I, n° 3223 ; IDEM, « Contre l'excessive distinction entre fichier et dossier – Le pas en avant du tribunal correctionnel de Paris », *Expertises*, 1990, pp. 16 et s.
Pour une application de cette distinction au domaine médical, voy. M. BOULANGER, S. CALLENS et S. BRILLON, « La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001 », *T. Gez.-Rev. dr. santé*, 2000-2001, pp. 327 et s.

À titre d'illustration n'ont pas été considérées comme constitutives d'un traitement de données au sens de la loi du 8 décembre 1992 les opérations effectuées sur les documents suivants sur support papier : des « lettres », des « rapports », des « courriers échangés avec le collège des anciens d'Esneux, avec ou entre les deux comités judiciaires » et « la réponse du bureau de la filiale ». « [T]ous documents qui ne font pas partie d'un "ensemble structuré" »[1]. Par ailleurs, la Cour d'appel de Bruxelles a estimé, dans un arrêt du 26 juin 2007, que « la simple mention du nom du propriétaire d'un immeuble sur l'affiche de vente d'un bien immobilier ne peut être considérée comme un traitement de données à caractère personnel dans un fichier [au sens de la loi du 8 décembre 1992] »[2].

Malgré leur appellation de « dossier » communément répandue, les dossiers de clients tenus par les avocats ou les médecins n'échappent, quant à eux, à la loi que dans l'hypothèse où les pièces rassemblées seraient exclusivement sur papier (ou microfiches ou bandes magnétiques) et ne font pas l'objet d'un classement permettant d'accéder de façon systématique aux données.

2.4 La notion de « Responsable du traitement »

Le rôle de responsable du traitement est essentiel dans la mesure où c'est à lui qu'incombe la majeure partie des obligations établies par la loi et c'est lui l'interlocuteur privilégié des personnes concernées par les données traitées. C'est à lui que ces dernières s'adresseront lorsqu'elles désireront exercer les droits que leur confère le régime de protection des données.

Il est donc impératif de déterminer qui est le responsable du traitement (appelé « maître du fichier » jusqu'à la révision de la loi en 1998).

2.4.1. Définition de la loi vie privée

La loi ne donne pas une réponse systématique à la question de la désignation du responsable. En revanche, elle fournit les critères permettant d'identifier ce dernier. Le responsable du traitement est « la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel »[3]. La loi précise également que, « lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est la personne physique, la personne morale, l'association de fait ou

1. Liège, 6 février 2006, *J.L.M.B.*, 2006, liv. 15, p. 665.
2. Bruxelles, 26 juin 2007, *R.W.*, 2008-2009, liv. 14, p. 578, notre traduction.
3. Article 1er, § 4, alinéa 1er.

l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance »[1].

L'alinéa 1er de l'article 1er, § 4, de la loi donne les trois critères permettant de désigner le responsable du traitement. Il s'agit du pouvoir de détermination des finalités et des moyens du traitement de données. Nous reviendrons sur chacun de ces critères dans les points c) et d) ci-dessous[2]. Dans l'exposé des motifs du projet de la future loi relative à la protection des données à caractère personnel du 11 décembre 1998, adaptant la loi belge de 1992 à la directive européenne en la matière, le ministre a précisé que c'est la personne investie du pouvoir de décision sur le traitement de données qui est visée par la notion de responsable du traitement[3].

2.4.2. Nature juridique

Il peut s'agir d'une personne physique ou morale ou même d'une association de fait.

Il convient de signaler qu'en dépit de la possibilité reconnue par la loi de désigner une association de fait comme responsable d'un traitement, il n'est pas nécessairement souhaitable de procéder de la sorte. En effet, si ne pas avoir de personnalité juridique propre n'empêche pas d'avoir la qualité de responsable de traitement, une telle solution conduit à des difficultés en cas de non-respect des dispositions de la loi, étant donné que la loi rend le responsable du traitement civilement, voire pénalement, responsable du non-respect. Il conviendra dans de tels cas de se tourner vers les personnes juridiquement responsables derrière l'écran de l'association de fait.

2.4.3. Le pouvoir de détermination

Le responsable du traitement est « responsable des choix qui président à la définition et à la mise en œuvre des traitements »[4].

Le Groupe de l'article 29 a considéré qu'« être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres »[5]. Il s'agira bien souvent d'une analyse factuelle. La désignation concrète des responsables de traitement est affaire de cas par cas. Au sein d'un cabinet d'avocats, par exemple, on sera attentif à l'organisa-

1. Article 1er, § 4, alinéa 2.
2. Pour une analyse approfondie illustrant l'application de ces critères en prenant le cas de Facebook, voy. J.-Ph. Moiny, « Facebook au regard des règles européennes concernant la protection des données », *R.E.C.O.-European Journal of Consumer Law*, 2010/2, pp. 247 et s.
3. Projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Exposé des motifs, *Doc. parl.*, Chambre, 1997-1998, n° 1566/1, p. 15.
4. M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreaux et Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p. 126.
5. Groupe de l'article 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », *WP* 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 9.

tion du cabinet (structure avec réseau commun, par exemple, ou juxtaposition d'activités individuelles indépendantes) pour être à même d'identifier les responsables des différents traitements de données.

Cela obligera le juge ou l'autorité de contrôle à vérifier si le responsable de traitement peut être considéré comme tel.

Le Groupe de l'article 29 ne dit rien d'autre en considérant que la capacité de déterminer « se déduira généralement d'une analyse des éléments factuels ou des circonstances de l'espèce : il conviendra d'examiner les opérations de traitement en question et de comprendre qui les détermine, en répondant dans un premier temps aux questions "pourquoi ce traitement a-t-il lieu ?" et "qui l'a entrepris ?"[1] ».

Une désignation erronée du responsable du traitement, c'est-à-dire qui est contredite par la situation de fait, ne lie pas le juge ni l'autorité de contrôle qui, dans une telle hypothèse, seront amenés à qualifier de responsable du traitement la personne répondant aux critères légaux.

2.4.4. La détermination des finalités et des moyens

Outre la capacité de déterminer, il faut qu'il y ait détermination des finalités et des moyens.

Selon le Groupe de l'article 29, « [o]n peut en outre affirmer que la détermination des finalités et des moyens revient à établir respectivement le "pourquoi" et le "comment" de certaines activités de traitement. Dans cette optique, et puisque ces deux éléments sont indissociables, il est nécessaire de donner des indications sur le degré d'influence qu'une entité doit avoir sur le "pourquoi" et le "comment" pour être qualifiée de responsable du traitement. [...] Lorsqu'il s'agit d'évaluer la détermination des finalités et des moyens en vue d'attribuer le rôle de responsable du traitement, la question centrale qui se pose est donc le degré de précision auquel une personne doit déterminer les finalités et les moyens afin d'être considérée comme un responsable du traitement et, en corollaire, la marge de manœuvre que la directive laisse à un sous-traitant. Ces définitions prennent tout leur sens lorsque divers acteurs interviennent dans le traitement de données à caractère personnel et qu'il est nécessaire de déterminer lesquels d'entre eux sont responsables du traitement (seuls ou conjointement avec d'autres) et lesquels sont à considérer comme des sous-traitants, le cas échéant »[2].

1. Groupe de l'article 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », *WP* 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 9.
2. Groupe de l'article 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », *WP* 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 14.

Par finalité, l'on entend l'objectif poursuivi par le responsable du traitement, le « pourquoi » évoqué par le Groupe de l'article 29.

Les moyens, pour leur part, expriment la façon par laquelle on atteindra l'objectif, la finalité, le « comment » évoqué par le Groupe de l'article 29. Ils peuvent être techniques, mais aussi organisationnels.

Au terme d'une telle analyse, la Cour d'appel de Mons a considéré qu'un détective privé devait être qualifié de responsable du traitement au motif qu'il a établi un rapport contenant des données à caractère personnel en utilisant un logiciel de traitement de texte[1]. Cette analyse est cependant contestable dès lors qu'un détective pourrait être considéré comme agissant pour le compte d'un tiers et sous ses instructions, caractéristiques d'un sous-traitant, ainsi que nous le verrons ci-dessous.

2.4.5. Les coresponsables du traitement

Il est à noter que la qualité de responsable du traitement peut être partagée et qu'il se peut que l'on désigne plusieurs coresponsables d'un traitement selon que plusieurs intervenants définissent les finalités ou les moyens de celui-ci.

2.5. La notion de « Sous-traitant »

Le sous-traitant est défini comme étant « la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données »[2].

Il ressort de cette définition que, pour être considéré comme sous-traitant, l'on ne peut pas être dans une relation hiérarchique avec le responsable du traitement et que l'on doit traiter des données à caractère personnel pour le compte de ce dernier.

Bien souvent, le sous-traitant interviendra au niveau des moyens à mettre en œuvre pour atteindre les finalités dès lors qu'il sera fait appel à lui pour ses compétences particulières. Ce sera le cas de fournisseurs de services Internet tels que les fournisseurs de *Cloud Computing*[3].

---

1. Mons (14e ch.), 2 mars 2010, *R.D.T.I.*, n° 41/2010, pp. 80 et s.
2. Article 1er, § 5.
3. Voy., à ce propos, J.-M. VAN GYSEGHEM, « *Cloud computing* et protection des données à caractère personnel : mise en ménage possible ? », *R.D.T.I.*, n° 42, pp. 35 à 50. Voy. également Groupe de l'article 29, avis 05/2012 sur l'informatique en nuage, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

À noter qu'une même personne peut être responsable de traitement dans le cadre d'un traitement et sous-traitant pour une autre.

3. Champ d'application *ratione materiae*

3.1. Conditions d'application de la loi

Aux termes de l'article 3, § 1er, de la loi du 8 décembre 1992, « la loi s'applique à tout traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ».

Toutes les données à caractère personnel évoquées ci-avant (au point 2.1.) ne sont donc couvertes par la loi que pour autant qu'elles fassent l'objet d'un traitement (voy. point 2.2.) entièrement ou partiellement automatisé. Les données à caractère personnel faisant l'objet d'un traitement non automatisé entrent également dans le champ d'application de la loi, mais seulement dans les cas où on est en présence d'un fichier (voy. point 2.3.).

3.1.1. Secteur public et secteur privé

Il importe de préciser d'emblée que les dispositions contenues dans la législation de protection des données à caractère personnel s'appliquent tant au secteur public qu'au secteur privé. Il est donc indifférent, pour la prise en compte des principes de protection des données, que le détenteur des informations soit une entité publique ou privée.

3.1.2. Recours à des moyens automatisés

La loi s'applique dès lors que recours est fait, à un moment ou à un autre, à des moyens automatisés. En clair, il suffit qu'une opération soit appliquée aux données en faisant intervenir, ne fût-ce qu'en partie, des moyens automatisés. Il suffit, par exemple, que les données soient au départ conservées sur un support informatisé et ensuite imprimées, ou qu'elles soient transmises en faisant usage de procédés automatisés, même si elles sont sur support papier (envoi par fax).

Les moyens automatisés englobent toutes les technologies de l'information et de la communication (TIC) : informatique, télématique, réseaux de télécommunication.

Il convient de faire remarquer que, quand interviennent des moyens automatisés, il ne faut pas obligatoirement que les données soient structurées d'une manière ou d'une autre pour que la loi s'applique. En effet, l'efficacité de tels moyens permet d'accéder à une ou plusieurs données enregistrées dans un ensemble (qui peut être une impressionnante base de données), de les sélectionner, les extraire, les associer, les modifier, etc. sans qu'il soit nécessaire que les données aient fait l'objet d'une structuration préalable pour arriver à ces résultats.

À titre d'illustration, des données à caractère personnel publiées de manière éparse (sur plusieurs pages différentes) et sans aucun ordre logique (pas par ordre alphabétique ou chronologique par exemple) sur un site Internet sont bel et bien couvertes par la législation de protection des données.

En cela, les traitements entièrement ou partiellement automatisés diffèrent des traitements dits « manuels ».

3.1.3. Traitements manuels

Dans l'hypothèse où aucun moyen automatisé n'intervient (en cas de données sur support papier, d'enregistrement sur bande magnétique ou de conservation sur microfiches), la loi devra quand même être respectée si les informations figurent ou sont destinées à figurer dans un fichier. Le fichier se caractérise, ainsi que dit plus haut, par la structuration des données personnelles qu'il contient permettant l'accessibilité de ces données.

En effet, c'est la facilité d'accès aux données qui est un des principaux facteurs de risques pour les droits et libertés des individus. Cette facilité est certes caractéristique des moyens automatisés, mais on la retrouve aussi, même si à un moindre degré, en présence de données rassemblées et conservées selon des critères de classement permettant précisément un accès direct aux données.

Les auteurs de la directive et, dans leur sillage, le législateur belge n'ont pas voulu qu'en ne visant que les moyens automatisés, ils suscitent la création de zones de non-protection pour des données qu'on consignerait dans des fichiers papier pour échapper aux règles légales.

La consultation de documents papier isolés ou l'envoi par courrier ordinaire de photocopies de documents papier qui ne sont pas extraits d'un « ensemble structuré de données à caractère personnel accessibles selon des critères déterminés » peuvent se faire, quant à eux, sans tenir compte des principes régissant la protection des données à caractère personnel.

Des exceptions à l'application de la loi sont prévues, soit globale, soustrayant certains traitements de données à l'ensemble de la loi, soit partielles, dispensant du respect de certaines dispositions de la loi seulement.

3.2. Exception intégrale à l'application de la loi pour les traitements à des fins personnelles ou domestiques

Bénéficient de l'exception globale du champ d'application de la loi vie privée les traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques[1].

Le considérant n° 12 de la directive 95/46 fournit deux exemples d'activités couvertes par cette exception : la correspondance et la tenue de répertoires d'adresses[2].

La justification de cette exclusion du champ d'application de la loi réside dans ce qu'on ne peut, au nom de la protection des données d'autrui, violer l'intimité de celui qui traite des données dans le cadre de sa vie privée et familiale, soit sa sphère personnelle.

La sphère personnelle peut être définie en faisant intervenir différents critères. Parmi ces critères, on trouve celui retenu par la Cour de justice de l'Union européenne dans son arrêt *Lindqvist*[3] et repris par la Cour à plusieurs reprises par la suite. La Cour de justice de l'Union européenne a commencé par dire que l'exception doit être interprétée comme « visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers »[4]. Elle a ensuite fait remarquer que ce « n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues acces-

1. Article 3, § 2, de la loi du 8 décembre 1992. Cette exception déjà présente dans la première version de la loi de 1992 est reprise, cette fois, en empruntant la formulation de l'article 3, § 2, de la directive 95/46.
2. Il est intéressant de relever que l'APEC Privacy Framework (instrument régional non contraignant de protection des données applicable aux pays membres de l'APEC) a introduit une restriction du même type à son champ d'application par le biais d'une exception apportée à la définition de *personal information controller*. Ainsi est exclu de cette définition tout individu « who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs » (APEC Privacy Framework, November 2004, disponible à l'adresse http://www.apec.org/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html, Part II Scope, § 10). Le commentaire de cette disposition apporte cet éclaircissement : « Individuals will often collect, hold and use personal information for personal, family or household purposes. For example, they often keep address books and phone lists or prepare family newsletters. The Framework is not intended to apply to such personal, family or household activities". La Résolution de Madrid, texte, issu d'un travail conjoint des autorités de protection des données de cinquante pays sous la houlette de l'Agence espagnole de la protection des données, admet, elle, que les lois nationales prévoient une exclusion du champ d'application pour les traitements réalisés par une personne physique dans le cadre d'activités exclusivement en lien avec sa vie privée ("private life") et familiale (Article 3, § 2) (*Madrid Resolution : Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the Processing of Personal Data*, disponible à l'adresse http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf.).
3. C.J.C.E., 6 novembre 2003 (Lindqvist), C-101-01, *Rec.*, p. I-12971, §§ 43 et 44.
4. C.J.C.E. (Lindqvist), préc., point 47.

sibles à un nombre indéfini de personnes ».[1] Le critère retenu est donc le fait de rendre les données accessibles à un nombre indéterminé de personnes.

La diffusion de données à caractère personnel sur un site Internet, sur un blog, sur une page Facebook ouverte à tous, sur un forum, sur Youtube, ne peut pas bénéficier de l'exception pour usage à des fins personnelles ou domestiques. Tous ces types de publication de données sont donc couverts par la législation de protection des données et doivent respecter les exigences de ce régime de protection.

En fait, ce sont « deux critères [qui] sont à prendre en compte : la nature de l'activité en cause et le "degré d'accessibilité de l'information" »[2].

La portée de cette exception doit tenir compte de changements majeurs apportés par Internet dans la délimitation des sphères publique et privée. La pertinence et la portée d'une telle exception ont pris ainsi une grande importance avec le développement du Web 2.0 et l'utilisation exponentielle de ses blogs, ses réseaux sociaux et son Twitter, par des particuliers qui fournissent désormais eux-mêmes des contenus dans lesquels figurent souvent des données à caractère personnel sous forme d'informations, de photos ou de vidéos. Recourir à ces médias est un moyen courant aujourd'hui pour s'exprimer, faire part de ses activités et de ses relations avec des tiers. C'est à la fois Internet comme lieu et moyen d'expression pour les individus en tant que citoyens et ce qu'on a appelé « le Web 2.0 pour les loisirs »[3]. Cet « Internet des loisirs » illustre parfaitement ce mélange de finalités personnelles et familiales et l'utilisation d'un mode public d'expression qui vient contredire la vocation « privée » des données partagées.

Cette réalité a pour conséquence qu'il n'est pas évident d'accepter ou de refuser purement et simplement l'application d'une exception telle celle qui est envisagée ici, dans le nouvel environnement technologique. Trouver un équilibre entre ne pas empiéter sur les activités personnelles des individus et néanmoins offrir une protection à autrui quand ces activités personnelles s'appuient sur des outils du Net est un véritable défi. Le défi est particulièrement patent lorsque l'on envisage l'application ou non de l'exception dans le cadre de l'usage des réseaux sociaux[4].

---

1. *Ibid.*
2. J.-Ph. Moiny, « Facebook au regard des règles européennes concernant la protection des données », *R.E.C.O.-European Journal of Consumer Law*, 2010/2, p. 251.
3. Discours « L'Internet du futur : l'Europe doit jouer un rôle majeur » de M^me^ Reding, Commissaire européenne DG Société de l'information et des Médias, à propos de l'initiative « Futur de l'Internet » du Conseil européen de Lisbonne (2 février 2009).
4. Sur ce point, pour une explication détaillée des cas où l'exception « à des fins personnelles et domestiques » joue dans le contexte des réseaux sociaux, voy. Groupe de l'article 29, avis 5/2009 du 12 juin 2009 sur les réseaux sociaux en ligne (*WP* 163) ; J.-Ph. Moiny, « Facebook au regard des règles européennes concernant la protection des données », *op. cit.*, pp. 250 et s.

3.3. Exceptions partielles à l'application de la loi

3.3.1. Exceptions pour les traitements de données à des fins journalistiques, artistiques ou littéraires

Les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire entrent, eux, dans la catégorie d'exceptions partielles. Une série de dispositions peuvent ne pas être appliquées à ces traitements, afin de garantir un équilibre avec la protection de la liberté d'expression[1].

a) Régime d'exemptions

Les personnes s'adonnant à des activités journalistiques sont incluses dans le champ de la loi, mais, à la différence de la situation issue de la première version de la loi de 1992[2], elles bénéficient d'un allégement de certaines règles. Il s'agit des règles dont l'application mettrait en péril la correcte exécution de la mission de la presse[3].

Levée de l'interdiction de principe de traiter des données sensibles, médicales et judiciaires

Dans les cas où l'on traite des données à caractère personnel aux seules fins de journalisme ou d'expression artistique ou littéraire, on est autorisé à traiter, dans deux hypothèses, des données qui normalement sont interdites de traitement sauf exceptions. Il s'agit des données sensibles visées à l'article 6 de la LVP, des données médicales évoquées à l'article 7 et des données judiciaires dont le sort est réglé à l'article 8 de la loi. Les données sensibles sont les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la vie sexuelle. Les données médicales sont les données relatives à la santé et couvrent tant la santé physique que la santé psychique. Quant aux données dites « judiciaires », il s'agit en fait des données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté.

Ainsi, aux termes de l'article 3, § 3, a), de la LVP, « [l]es articles 6, 7 et 8 ne s'appliquent pas aux traitements de données à caractère personnel effectués aux seules

1. Article 3, § 3, de la loi du 8 décembre 1992.
2. Le régime antérieur qui ne mettait pas en place un tel régime allégé avait d'ailleurs suscité inquiétudes et critiques. Voy. M. FLAMME et TH. LÉONARD, « La liberté de la presse à l'aune de la protection des données : liberté responsable ou liberté surveillée ? », *R.G.D.C.*, 1997, pp. 5 à 42.
3. Pour une réflexion sur la situation mise en place et les conséquences délicates pour les journalistes, voy. TH. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, pp. 380 et 381.

fins de journalisme ou d'expression artistique ou littéraire lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou sur des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée ».

Les deux hypothèses dans lesquelles ces trois catégories particulières de données peuvent être traitées à des fins de journalisme ou d'expression artistique ou littéraire sont donc :

- les situations dans lesquelles la personne concernée par les données a elle-même rendu celles-ci publiques (le fait pour un candidat aux élections de divulguer nécessairement son opinion politique lors d'une campagne électorale, par exemple, ou le fait d'avoir participé à une manifestation syndicale en arborant les couleurs d'un syndicat, etc.) ;
- les situations dans lesquelles les données particulières se rapportent à une personne publique (personne politique, responsable religieux, personnalités sportives, célébrités...) et sont en lien direct avec le caractère public de cette personne ; ou lorsque les données sont en relation étroite avec un fait public (p. ex., fait de l'actualité judiciaire) dans lequel la personne concernée est impliquée.

Exemption de l'obligation d'information des personnes concernées

Comme on le verra ultérieurement, le responsable du traitement est normalement tenu de fournir certaines informations à la personne concernée auprès de qui il collecte des données. Si le traitement des données poursuit une finalité de journalisme ou d'expression littéraire ou artistique, cette obligation tombe, mais seulement dans le cas où fournir l'information obligatoire risquerait de compromettre la collecte des données. L'article 3, § 3, b), de la LVP dispose en ce sens que « [l]'article 9, § 1er, ne s'applique pas aux traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire lorsque son application compromettrait la collecte des données auprès de la personne concernée ».

Si la collecte ne s'effectue pas directement auprès de la personne concernée, mais auprès de sources indirectes, l'article 9, § 2, de la LVP prévoit également une obligation d'information dans le chef du responsable du traitement. Cette obligation est elle aussi levée en cas de traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, mais seulement au cas où « son application aurait une ou plusieurs des conséquences suivantes :

- son application compromettrait la collecte des données ;
- son application compromettrait une publication en projet ;
- son application fournirait des indications sur les sources d'information »[1].

1. Article 3, § 3, b), alinéa 2, de la loi du 8 décembre 1992.

Suppression des droits d'accès, de rectification et d'opposition des personnes concernées

Le droit d'accès aux données accordé par l'article 10 de la loi aux personnes concernées, de même que les droits de rectification des données et d'opposition au traitement, reconnus à l'article 12, peuvent ne pas être accordés à la personne concernée, mais seulement « dans la mesure où leur application compromettrait une publication en projet ou fournirait des indications sur les sources d'information »[1].

Suppression du régime des flux transfrontières de données

Les personnes traitant des données à des fins journalistiques, littéraires ou artistiques sont dispensées de manière systématique et généralisée de respecter les exigences de protection liées aux situations de flux transfrontières de données, c'est-à-dire lorsque les données sont destinées à franchir les frontières de l'Union européenne et de l'Espace économique européen.

Selon l'article 3, § 3, d), de la LVP, « les articles [...] 21 et 22 [mettant en place le régime des flux transfrontières] ne s'appliquent pas aux traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire ».

Suppression de la publicité des traitements via le registre public

Enfin, quelques allégements sont admis dans la déclaration des traitements qui doit être effectuée auprès de la Commission de la protection de la vie privée[2]. Mais, surtout, à la différence de toutes les déclarations de traitements, celles concernant des traitements de données à des fins journalistiques, artistiques ou littéraires ne doivent pas figurer dans le registre public tenu par la Commission.

b) Notion de traitement à des fins journalistiques

Dès le processus de transposition de la directive 95/46 du 24 octobre 1995 relative à la protection des données à caractère personnel[3] en droit belge, au sein de la loi vie privée, les intervenants ont relevé la difficulté qu'il y avait à cerner précisément les

1. Article 3, § 3, c), de la loi du 8 décembre 1992.
2. Article 3, § 3, d), de la loi du 8 décembre 1992.
3. Directive (CE) 95/46 du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.U.E.*, L 281, p. 31. L'article 9, intitulé « Traitements de données à caractère personnel et liberté d'expression », dispose : « Les États membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression. »

notions utilisées dans cette exception[1]. C'est à la Cour de justice des Communautés européennes qu'il revenait de clarifier ces notions découlant d'une directive européenne, qui laissaient perplexe une grande partie de la doctrine spécialisée en matière de protection des données.

Si la notion de « traitement à des fins littéraires ou artistiques » n'a pas encore été élucidée, une affaire finlandaise[2], comme l'indique le nom des parties (ardu pour les non-praticiens des langues finno-ougriennes...), a donné à la Cour de justice de Luxembourg l'occasion d'apporter les éclaircissements souhaités quant à la notion de « traitement de données à caractère personnel effectué aux seules fins de journalisme » apparaissant à l'article 9 de la directive 95/46 et reprise dans la loi belge. La Cour a en effet été invitée à répondre à des questions préjudicielles mettant en jeu cette deuxième notion[3].

Notion de journalisme dans le contexte d'Internet

A priori limpide, cette notion a perdu de sa clarté une fois placée dans le contexte d'Internet, et des interrogations concernant sa portée et son contour précis dans ce nouvel environnement se sont rapidement fait jour.

La notion de « traitement à des fins journalistiques » n'est en effet pas centrée sur un acteur (les médias), mais sur une activité (le journalisme). Or on a dû constater que, dans la sphère Internet, cette activité n'était plus l'apanage d'organes de presse bien établis et reconnus comme tels ou de journalistes patentés détenteurs d'une carte de presse. Peu à peu se sont développés des sites Web d'organisations et d'associations désireuses de mettre en lumière certaines informations ou de réagir à certaines actualités[4]. De même, des blogs personnels sont apparus par lesquels des individus publient à leur tour des informations qu'ils assortissent de commentaires personnels et qu'ils partagent avec un public invité à manifester ses réactions.

1. Ainsi, le Conseil d'État avait expressément demandé au législateur d'apporter des précisions sur ce qu'il faut entendre par « fins de journalisme » et « fins d'expression littéraire et artistique » (avis du Conseil d'État, pp. 186 à 188). Ce que le législateur a refusé de faire étant donné qu'il s'agit de notions découlant d'une directive européenne et, partant, appelées à être éclairées par la Cour de justice de l'Union européenne.
2. C.J.C.E., 16 décembre 2008 (Tietosuojavaltuutettu c. Satakunnan markkinapörssi oy et Satamedia oy), C-73/07.
3. Sur cette affaire, voy. C. DE TERWANGNE, « Les dérogations à la protection des données en faveur des activités de journalisme enfin élucidées », note sous C.J.C.E. (Gr. Ch.), 16 décembre 2008 (Satakunnan Markkinapörssi Oy et Satamedia Oy), aff. C-73/07, *R.D.T.I.*, 2010, n° 38, pp. 132 à 146.
4. Il est intéressant d'observer que la Cour européenne des droits de l'homme a décidé d'élargir la protection accordée à la presse à ceux qui « font œuvre de presse » (C. SCHÖLLER, « Liberté d'expression. Jurisprudence de la Cour européenne des droits de l'homme », *in* C. DE TERWANGNE et S. DUSOLLIER (coord.), *Chronique de jurisprudence en droit des technologies de l'information (2002-2008), R.D.T.I.*, 2009, n° 35, p. 116). Voy. notamment Cour eur. D.H., arrêt Vides Aizsardzibas Klubs c. Lettonie, 27 mai 2004, req. n° 57829/00, § 42 : « En tant qu'organisation non gouvernementale spécialisée en la matière, la requérante a donc exercé son rôle de "chien de garde" [...]. Une telle participation d'une association étant essentielle pour une société démocratique, la Cour estime qu'elle est similaire au rôle de la presse tel que défini par sa jurisprudence constante » ou, encore, Cour eur. D.H., arrêt Steel et Morris c. Royaume-Uni, 15 février 2005, req. n° 68416/01, § 89 (voy. *infra*).

Aujourd'hui, les réseaux sociaux et les moyens de télécommunications mobiles ont également pris le relais dans la diffusion d'informations et c'est via Facebook ou Twitter, par exemple, que certains, professionnels ou quidams, éminents spécialistes ou simples témoins, diffusent désormais dans le public des informations, des commentaires, des films ou des photos liées à l'actualité[1].

Dans quelle mesure toutes ces hypothèses doivent-elles être comprises comme étant des activités poursuivant des « fins de journalisme » ? C'est dire que l'on attendait avec intérêt une clarification de la part de la Cour de justice sur cette question.

Définition large de la Cour

La Cour estime que l'importance de la liberté d'expression impose d'interpréter de manière large la notion de journalisme, afférente à cette liberté[2]. En contrepartie, la juste pondération des droits sera réalisée par le fait que seules les dérogations et limitations de la protection des données strictement nécessaires sont admises[3].

Dans la ligne de cette position claire en faveur d'une interprétation large de la notion de journalisme, la Cour a mis au jour plusieurs éléments qui donnent la pleine mesure de ce qu'elle entend par « interprétation large ».

Éléments intervenant dans la notion d'activité de journalisme

La Cour a tout d'abord précisé que les exemptions et dérogations prévues à l'article 9 ne sont pas réservées aux seules entreprises de média[4]. Les travaux préparatoires de la directive indiquent clairement que le régime dérogatoire est destiné à bénéficier à « toute personne exerçant une activité de journalisme »[5].

Ensuite, la Cour a observé, à l'instar des sociétés parties au litige et de l'avocate générale, que, légitimement, toute entreprise, y compris celles poursuivant des activités de journalisme, cherche à obtenir un profit de son activité. Dans certains cas, « un certain succès commercial peut même constituer la condition *sine qua non* de la

1. L'expérience « Huis clos sur le Net », en février 2010, a vu cinq journalistes des radios francophones publiques, isolés dans un gîte rural pendant une semaine. Coupés de tous les médias traditionnels, ces journalistes avaient pour seul accès à l'information Facebook et Twitter. Cette expérience était destinée à faire réfléchir à l'émergence de l'information sur les réseaux sociaux. Voy. « "Huis clos sur le Net" : une opération inédite », France Info, 21 janvier 2010, à l'adresse http://www.france-info.com/culture-medias-2010-01-21-huis-clos-sur-le-net-une-operation-inedite-394976-36-41.html.
2. § 56 de l'arrêt.
3. *Ibid.*
4. § 58 de l'arrêt.
5. Voy. notamment PARLEMENT EUROPÉEN, avis du 11 mars 1992, *J.O.*, C 94, p. 173 ; COMMISSION EUROPÉENNE, proposition modifiée du 15 octobre 1992, *J.O.*, C 311, p. 30 ; CONSEIL, position commune du 20 février 1995, *J.O.*, C 93, p. 1.

subsistance d'un journalisme professionnel »[1]. En conséquence, poursuivre des fins lucratives ne dénature pas l'activité de journalisme[2].

Troisièmement, il s'impose pour la Cour de prendre en compte l'évolution des moyens de communication et de diffusion des informations. Rejoignant les remarques émises notamment par le gouvernement suédois intervenu dans la procédure, la Cour déclare que la qualification d'activités de journalisme est indépendante du support utilisé pour transmettre les informations. Ainsi, que ce support soit « classique tel que le papier ou les ondes hertziennes, ou électronique tel que l'Internet, » n'est pas déterminant[3].

La Cour a, jusque-là, pris la peine de préciser de manière étayée trois éléments qui sont liés à la notion de journalisme sans être au cœur même de cette notion. Elle a porté son attention sur la question de savoir qui exerce l'activité, comment et avec un but de lucre ou non. Elle n'a pas apporté d'éclaircissement sur ce qui caractérise l'activité de journalisme en elle-même.

Ce qui est étonnant, c'est que ce cœur de la notion, la Cour l'énoncera dans son paragraphe récapitulatif sans aucun développement ni explication. Elle conclut ainsi qu'« il découle de tout ce qui précède que des activités [...] peuvent être qualifiées d'"activités de journalisme", *si elles ont pour finalité la divulgation au public d'informations, d'opinions ou d'idées*, sous quelque moyen de transmission que ce soit. Elles ne sont pas réservées aux entreprises de média et peuvent être liées à un but lucratif »[4].

Dans la formulation de sa réponse à la question soulevée par la juridiction administrative finlandaise, la Cour ne reprendra d'ailleurs plus que cet élément central. Elle énonce que « les activités [...] doivent être considérées comme des activités de traitement de données à caractère personnel exercées "aux seules fins de journalisme" au sens de [l'article 9 de la directive], si lesdites activités ont pour seule finalité la divulgation au public d'informations, d'opinions ou d'idées »[5]. C'est donc le seul fait

1. §. 59 de l'arrêt. Également point 82 des conclusions de l'avocate générale (concl. Av. gén. M^me^ Juliane Kokott du 8 mai 2008 dans l'affaire *Satakunnan Markkinapörssi Oy et Satamedia Oy*, C-73/07).
2. Cette position est contraire à celle adoptée par les États généraux de la presse écrite en France, pour la notion d'éditeur de presse. Voy. le Livre vert, 8 janvier 2009, disponible à l'adresse http://www.etatsgenerauxdelapresseecrite.fr/lenjeu/?lang=fr, recommandations du Pôle « Le choc d'Internet. Quels modèles pour la presse écrite » : « Proposition 4 – Reconnaître un statut d'éditeur de presse en ligne qui n'exclut aucune des formes numériques ni aucun des supports utilisés actuellement et à l'avenir. Ce statut spécifique d'éditeur de presse en ligne repose sur les trois critères cumulatifs suivants :
   - Critère 1 : exercice d'une mission d'information à titre professionnel à l'égard du public ;
   - Critère 2 : production et mise à disposition du public de contenu original, composé d'informations ayant fait l'objet d'un traitement journalistique et présentant un lien avec l'actualité, *sans constituer, en lui-même, un outil de promotion ou un accessoire d'une activité industrielle ou commerciale* ;
   - Critère 3 : emploi régulier de journalistes professionnels dans l'activité des entreprises concernées, dans le cadre des règles sociales et déontologiques de la profession. » (Nous soulignons.)
3. §. 60 de l'arrêt.
4. § 61 de l'arrêt (c'est nous qui soulignons).
5. § 62 de l'arrêt.

que des activités visent la communication au public qui est décisif pour qualifier les activités de « journalistiques ». On conviendra que c'est particulièrement large et on ne voit pas vraiment ce qui pourrait différencier cette définition de l'exercice de la liberté d'expression pure et simple.

La Cour ne fait aucun écho aux longs développements consacrés par son avocate générale à la mise au jour d'une définition affinée qui prendrait en compte la mission des médias dans une société démocratique. Cette mission consiste à communiquer des informations et des idées sur toutes les questions d'intérêt public[1]. Pour M^me^ Kokott, de même que pour le gouvernement suédois, un traitement de données doit en conséquence être considéré comme effectué à des fins de journalisme « lorsqu'il vise la communication d'informations et d'idées sur des questions d'intérêt public »[2]. L'avocate générale éprouve cependant quelque peine à déterminer ce qu'il faut entendre par question d'intérêt public. Elle spécifie qu'il y a un intérêt public quand les informations se rattachent à un débat public ayant (eu) cours ou quand elles portent sur des questions d'intérêt public par nature en fonction des valeurs sociales. Toutefois, les médias pouvant susciter l'intérêt public par la diffusion même d'informations, on ne peut donc estimer *a priori* que la question n'est pas/ne sera pas d'intérêt public. L'avocate générale débouche alors sur une conclusion qui laisse un peu sur sa faim : « Par conséquent, on ne peut constater que la diffusion d'informations et d'idées ne concerne pas des questions d'intérêt public que lorsque cela devient évident »[3]. Ce n'est certes pas très opérationnel comme critère…

Est-ce cette difficulté qui rebutera la Cour et l'incitera à abandonner toute référence à l'intérêt public ? La Cour n'est en rien explicite sur ce point et les commentateurs sont laissés à leurs conjectures[4].

3.3.2. Exceptions pour les traitements de données par les services de sécurité et de renseignement

D'autres exceptions partielles, pour classiques qu'elles soient, sont particulièrement larges. Il s'agit des exceptions accordées aux traitements effectués à des fins de sécurité publique[5].

Il est étonnant et particulièrement dommage que ces exceptions n'aient fait l'objet d'aucun débat au sein de la société ou, à tout le moins, au sein du Parlement, au moment de leur adoption. D'autant que « la loi consacre un dangereux déséquilibre entre les impératifs légitimes de la sécurité de l'État et de sa défense et les intérêts de

1. Concl., préc., point 66 et les références citées des arrêts de la Cour européenne des droits de l'homme en ce sens.
2. Concl., préc., point 69.
3. Concl., préc., point 78.
4. Pour un commentaire sur la pertinence ou non de l'approche de la Cour de justice de l'Union européenne dans cette affaire, voy. C. DE TERWANGNE, « Les dérogations à la protection des données en faveur des activités de journalisme enfin élucidées », *op. cit.*, n° 6.
5. Article 3, §§ 4 et 5, de la loi du 8 décembre 1992.

la personne concernée dans la mesure où la loi affaiblit de manière disproportionnée les possibilités de contrôle du respect des prérogatives liées à la protection des données »[1].

a) Régime dérogatoire

Les dérogations accordées pour les autorités en charge de la sûreté touchent la majorité des dispositions protectrices de la loi vie privée[2].

Certaines dispositions cruciales demeurent toutefois d'application. Il s'agit essentiellement :

- des dispositions énonçant les principes de base de la licéité d'un traitement : principes de loyauté, de finalité (interdisant notamment les utilisations de données non compatibles et imposant une durée de conservation limitée, voy. *infra*), de proportionnalité, règle de qualité des données ;
- du droit d'accès indirect à exercer via l'intermédiaire de la Commission de la protection de la vie privée ;
- des obligations en termes de sécurité ;
- des règles limitatives pour les flux transfrontières de données.

On relève cependant que l'instauration d'un droit d'accès indirect en lieu et place d'un droit direct d'accès et de consultation des données traitées par les autorités en charge de la sûreté et du renseignement revient à instaurer une exception systématique au droit d'accès dans ces hypothèses. Ce système d'exception absolue est contraire à l'article 13 de la directive qui admet des exceptions aux droits accordés, mais seulement dans la mesure où cela est « nécessaire » à la sauvegarde d'intérêts supérieurs[3]. L'exigence de nécessité implique, dans la ligne de la jurisprudence de la Cour européenne des droits de l'homme, que soit vérifié dans chaque cas le respect de la proportionnalité et de l'efficacité de la mesure[4].

b) Autorités bénéficiaires de l'exception

À la différence de la démarche adoptée pour définir l'exception précédente, le législateur ne cerne pas cette exception-ci en fonction de la finalité des activités menées, mais plutôt en fonction des autorités effectuant certains traitements de données.

---

1. Y. POULLET et B. HAVELANGE, « Secrets d'État et vie privée ou comment concilier l'inconciliable ? », *in Droit des Technologies de l'information. Regards prospectifs*, coll. Cahiers du CRID, n° 16, Bruxelles, Bruylant, 1999, n° 15.
2. Les articles 6 à 10, 12, 14, 15, 17, 17*bis*, alinéa 1er, 18, 20 et 31, §§ 1er à 3, ne s'appliquent pas.
3. Article 13 de la directive 95/46 : « Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6, paragraphe 1, à l'article 10 [droit d'accès], à l'article 11, paragraphe 1, et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder :
   a) la sûreté de l'État ;
   b) la défense ;
   c) la sécurité publique ; [...]. »
4. B. HAVELANGE et Y. POULLET, « Secrets d'État et vie privée ou comment concilier l'inconciliable ? », *op. cit.* p. 390.

Cette technique législative a pour conséquence que l'apparition de toute nouvelle autorité à qui sont confiées des compétences en matière de sécurité et de renseignement conduit à une modification de la liste de la loi du 8 décembre 1992 afin de faire bénéficier cette nouvelle autorité du régime dérogatoire.

Telle qu'elle figure à l'article 3, § 4, de la LVP, la liste des autorités dont les traitements de données à caractère personnel nécessaires à l'exercice de leur mission sont couverts par l'exception comprend aujourd'hui : la Sûreté de l'État, le Service général du renseignement et de la sécurité des forces armées, les autorités visées aux articles 15, 22*ter* et 22*quinquies* de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité et l'organe de recours créé par la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité, les officiers de sécurité et le Comité permanent de contrôle des services de renseignements et son Service d'enquêtes, ainsi que l'Organe de coordination pour l'analyse de la menace.

3.3.3. Exceptions pour les traitements de données par les autorités en charge de missions de police judiciaire et administrative

Les services et autorités en charge de missions de police judiciaire ou administrative sont presque entièrement soumis à la loi vie privée. Seules les dispositions instaurant la transparence des traitements de données sont déclarées inapplicables à l'activité de ces services[1]. Il est clair que de telles mesures de transparence iraient à l'encontre d'une action efficace des services de police.

Ces services sont dispensés de l'obligation de transparence spontanée consistant à informer les personnes concernées du traitement qui est effectué, impliquant des données les concernant (art. 9 de la loi).

La transparence réalisée à travers l'octroi de droits aux personnes concernées est également neutralisée. Le droit d'accès aux données et de rectification des données erronées ou incomplètes est supprimé. La remarque soulevée ci-dessus sur la non-conformité de ces exceptions absolues aux droits des personnes concernées au

1. Article 3, § 5, LVP : « Les articles 9, 10, § 1er, et 12 ne s'appliquent pas :
1° aux traitements de données à caractère personnel gérés par des autorités publiques en vue de l'exercice de leurs missions de police judiciaire ;
2° aux traitements de données à caractère personnel gérés par les services de police visés à l'article 3 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements, en vue de l'exercice de leurs missions de police administrative ;
3° aux traitements de données à caractère personnel gérés en vue de l'exercice de leurs missions de police administrative, par d'autres autorités publiques qui ont été désignées par arrêté royal délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée ;
4° aux traitements de données à caractère personnel rendus nécessaires par la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ;
5° au traitement de données à caractère personnel géré par le Comité permanent de contrôle des services de police et par son Service d'enquêtes en vue de l'exercice de leurs missions légales. »

regard de l'article 13 de la directive 95/46 ainsi que de la jurisprudence de la Cour européenne des droits de l'homme est également valide ici.

3.3.4. Exceptions pour les traitements de données par Child Focus

Un régime d'exceptions a été réservé au Centre européen pour enfants disparus et sexuellement exploités, couramment appelé le centre Child Focus.

On regrettera avec d'autres auteurs[1] la place disproportionnée accordée à cette exception particulière dans les débats parlementaires qui ont conduit à la transposition de la directive dans la loi de 1992.

3.3.5. Exceptions pour les traitements de données par le SPF Finances

Une nouvelle exception partielle a été introduite par une modification de la loi vie privée intervenue le 3 août 2012. Elle concerne les dispositions instaurant la transparence des traitements de données, dans le contexte des activités de contrôle ou d'enquête du SPF Finances.

À l'instar de l'exception relative aux activités de police, le SPF Finances est soustrait à l'obligation de transparence spontanée consistant à informer les personnes concernées du traitement qui est effectué, impliquant des données les concernant (art. 9 de la loi).

La transparence réalisée à travers l'octroi de droits aux personnes concernées est ici aussi neutralisée. Le droit d'accès aux données et de rectification des données erronées ou incomplètes est supprimé.

Dans un souci de réduire l'atteinte aux règles de protection, cette exception est cependant limitée dans le temps. Elle n'est valable que durant la période durant laquelle est effectué un contrôle ou une enquête.

Un paragraphe 7 supplémentaire a été ajouté à la liste des exceptions, ainsi rédigé :

> « § 7. Les articles 9, § 2, 10 et 12 ne sont pas applicables aux traitements de données à caractère personnel gérés par le Service public fédéral Finances durant la période dans laquelle la personne concernée est l'objet d'un contrôle ou d'une enquête ou d'actes préparatoires à ceux-ci effectués par le Service public fédéral Finances dans le cadre de l'exécution de ses missions légales.
> Lorsque le Service public fédéral Finances a fait usage de l'exception telle que déterminée à l'alinéa premier, la règle de l'exception est immédiatement levée après la clôture du contrôle ou de l'enquête. Le Service de Sécurité de l'Informa-

1. P. De Hert et D. Pissoort, *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2004, pp. 81 et 82.

tion et Protection de la Vie Privée en informe le contribuable concerné sans délai. »

4. Champ d'application *ratione loci*

Le législateur belge, suivant la directive, a modifié le critère de rattachement conduisant à l'applicabilité de la loi.

Relevons d'emblée que ni la nationalité des personnes concernées ni leur lieu de résidence habituelle ni la localisation physique des données à caractère personnel ne sont déterminants pour décider de l'application de la loi belge à une situation de traitement de données.

Les critères à prendre en considération pour déterminer si la loi belge est applicable sont le lieu d'établissement du responsable du traitement (critère principal) et, dans le cas où ce responsable se trouverait en dehors de l'Union européenne, la localisation des moyens utilisés (critère secondaire)[1].

4.1. Critère de rattachement principal : le lieu d'établissement du responsable du traitement

Le législateur s'est définitivement écarté de la notion de « fichier », déterminante dans les premières générations de législations en la matière et basée sur une localisation physique précise des données (sur une disquette, sur le disque dur d'un ordinateur identifié...). Il n'a plus retenu non plus la localisation du traitement, celui-ci pouvant désormais être effectué sur des données qui ne sont pas rassemblées dans un « lieu » unique.

C'est le *lieu d'établissement fixe*[2] *du responsable du traitement* qui est à présent le critère d'applicabilité de la loi[3]. La loi vie privée s'applique lorsque les données sont traitées dans le cadre des activités d'un établissement fixe du responsable du traite-

1. Sur la question du droit applicable, voy. les développements fouillés et les nombreux exemples très éclairants dans l'avis du Groupe de l'article 29, avis 8/2010 du 16 décembre 2010 sur le droit applicable, *WP* 179.
2. Le considérant n° 19 de la directive 95/46/CE précise que « l'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. [...] La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à ce sujet ».
3. Article 3*bis*, alinéa 1er, 1°, de la loi du 8 décembre 1992.

ment localisé sur le territoire belge[1]. L'établissement sur le sol belge suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable.

La forme juridique d'un tel établissement importe peu. Il peut s'agir d'une simple succursale, d'un bureau local, d'une filiale possédant la personnalité juridique ou d'une agence tierce[2]. Un serveur ou un ordinateur ne sont, quant à eux, pas susceptibles d'être qualifiés d'établissements, « puisqu'il s'agit simplement d'une installation technique ou d'un outil de traitement d'informations »[3].

Toutefois, le traitement doit être effectué « dans le cadre des activités de l'établissement ». L'établissement du responsable du traitement doit participer à des activités impliquant le traitement de données à caractère personnel. Cela signifie que « l'établissement doit également jouer un rôle significatif dans l'opération de traitement en question »[4]. À cet égard, « il convient de prendre en considération le degré de participation de l'établissement aux activités de traitement, la nature des activités, ainsi que la nécessité d'assurer la protection effective des données »[5].

Ainsi, si un complexe hôtelier localisé en Belgique offre un service de réservation via Internet et demande en conséquence aux intéressés d'enregistrer leurs coordonnées afin d'effectuer la réservation, la loi belge de protection des données trouvera à s'appliquer au traitement de ces informations. Un cabinet d'avocats faisant partie d'une structure « internationale » présente dans plusieurs États devra, quant à lui, tout de même respecter la loi belge pour les activités déployées dans l'entité établie sur le territoire belge. La dépendance de ce cabinet à l'égard d'une entité mère ou son intégration complète dans une société de droit étranger est sans incidence sur la règle d'application de la loi belge de protection des données.

> « Le lieu d'établissement d'une société qui fournit des services par le biais d'un site Internet n'est pas le lieu où est située la technologie qui supporte son site web ni le lieu d'accès au site Web mais le lieu où elle exerce son activité »[6].

1. … ou en un lieu où la loi belge s'applique en vertu du droit international public (art. 3*bis* de la loi).
2. Considérant n° 19 de la directive 95/46.
3. Groupe de l'article 29, avis sur le droit applicable, préc., p. 13.
4. Groupe de l'article 29, avis 1/2008 du 4 avril 2008 sur les aspects de la protection des données liés aux moteurs de recherche, *WP* 148.
5. Groupe de l'article 29, avis 8/2010 du 16 décembre 2010 sur le droit applicable, *WP* 179.
6. Groupe de l'article 29, document de travail du 30 mai 2002 sur l'application internationale du droit de l'Union européenne en matière de protection des données au traitement de données à caractère personnel sur Internet par des sites Web établis en dehors de l'Union européenne, *WP* 56.

4.2. Critère de rattachement secondaire : le recours à des moyens localisés sur le territoire belge

4.2.1. Présentation du critère

À l'instar du législateur européen, le législateur belge s'est préoccupé des tentatives de contournement du régime de protection mis en place par la délocalisation de l'établissement du responsable du traitement[1]. Il a dans le même temps manifesté son souci que les traitements de données présentant un lien étroit avec notre territoire, mais effectués par un responsable se situant en dehors des frontières, ne se retrouvent pas dépourvus de protection[2].

Afin d'éviter pareille situation, l'article 3*bis* de la loi du 8 décembre 1992[3] prévoit que tout responsable qui n'est pas établi de manière permanente sur le territoire de la Communauté européenne, mais qui recourt à des moyens, automatisés ou non, situés sur le territoire belge, dans le but de traiter des données personnelles, est soumis à cette loi. Il est tenu, en outre, de désigner un représentant établi sur le territoire belge[4].

Le seul transit de données sur le territoire belge n'est toutefois pas couvert par la loi.

L'Exposé des motifs de la loi du 11 décembre 1998 signale que « le terme "moyens" recouvre tout équipement possible, tels les ordinateurs, les appareils de télécommunications, les unités d'impression, etc., à l'exclusion, formulée explicitement, des moyens qui sont uniquement utilisés pour le transit des données à caractère personnel par le territoire, tels que les câbles, les routeurs, etc. »[5].

Pour reprendre l'exemple du cabinet d'avocats à dimension multinationale repris ci-dessus, la désignation d'un responsable du traitement localisé à l'étranger, mais recueillant des données en Belgique en utilisant des moyens situés dans le pays, par exemple en ayant accès via un réseau électronique aux données concernant les associés ou les collaborateurs du cabinet, ne permettra donc pas d'échapper à la loi belge.

---

1. Voy. considérant n° 20 de la directive 95/46 : « considérant que l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive ; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'État membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés ».
2. Voy. Groupe de l'article 29, avis sur le droit applicable, préc., p. 21.
3. Article 3*bis*, alinéa 1er, 2°, de la loi du 8 décembre 1992.
4. Article 3*bis*, alinéa 2, de la loi du 8 décembre 1992.
5. Exposé des motifs, *Doc. parl.*, Chambre, 1997-1998, n° 1566/1, p. 27. Voy. J. DUMORTIER, « De nieuwe wetgeving over de verwerking van persoonsgegevens », *Recente ontwikkelingen in informatica- en telecommunicatierecht*, Brugge, die Keure, 1999, p. 85, spéc. note 33.

4.2.2. Difficulté d'application dans le contexte d'Internet

Dans le monde en réseau que nous connaissons, et principalement dans le contexte d'Internet, une lecture littérale de ce deuxième critère de rattachement légal conduit à une situation impraticable. Elle impliquerait, en effet, d'étendre l'application de la loi belge à tout utilisateur d'Internet qui copie ou télécharge des informations nominatives à partir d'un site Web ouvert par un fournisseur d'informations établi en Belgique[1]. Ce faisant, l'internaute effectuerait en effet un traitement de données en recourant à des moyens automatisés situés en Belgique. Il serait donc tenu de respecter la loi belge et de désigner un représentant établi dans notre pays. Il en irait de même pour tout responsable de site Web de par le monde qui invite les internautes, via le site, à communiquer des informations nominatives. Lorsqu'un internaute communique ses données par des moyens situés sur le territoire belge (son ordinateur, les installations de son fournisseur d'accès, les appareils de télécommunications), la collecte réalisée par le responsable du site serait soumise à la loi belge et le responsable devrait désigner un représentant en Belgique. Ce serait assurément irréaliste.

Pour garder à l'article 3*bis* une portée effective, la seule lecture de cette disposition qui s'impose est une lecture téléologique. La *ratio legis* de cet article se résume clairement dans la volonté d'éviter que les individus se retrouvent dépourvus de toute protection, en particulier du fait d'un contournement de la législation[2]. Le souci des auteurs du texte est donc d'assurer une protection à ceux qui doivent normalement en bénéficier sous l'égide de la loi, même en dehors des frontières.

C'est par une lecture combinée de l'article 3*bis* et des articles 21 et 22 qui régissent les flux transfrontières vers les États non membres de l'Union européenne qu'une définition rationnelle de l'applicabilité de la loi peut être dégagée.[3]

On peut en effet considérer qu'une première réponse à la préoccupation du législateur est donnée par l'instauration d'un régime protecteur en matière de flux transfrontières de données en dehors de l'Union européenne. Dans le cadre de la réglementation de ces flux, les exigences édictées par la loi s'imposent à tous les acteurs qui effectuent des opérations sur des données transférées à partir de la Bel-

1. Sur le raisonnement attaché à cet exemple, voy. M.-H. BOULANGER et C. DE TERWANGNE, « Internet et le respect de la vie privée », *in Internet face au droit*, coll. Cahiers du CRID, n° 12, Bruxelles, Story-Scientia, 1997, pp. 201 et 202.
2. Voy. l'exposé des motifs (*Doc. parl.*, Chambre, 1997-1998, n° 1566/1, p. 27) et le considérant n° 20 de la directive.
3. Le raisonnement exposé dans les paragraphes qui suivent a été développé par M.-H. BOULANGER et C. DE TERWANGNE, « Internet et le respect de la vie privée », *in Internet face au droit*, coll. Cahiers du CRID, n° 12, Bruxelles, Story-Scientia, 1997, pp. 201 et 202. La doctrine s'est ralliée à cette interprétation : voy. notamment TH. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 383 ; Y. POULLET, « Internet et Vie privée : entre risques et espoirs », *J.T.*, 2001, pp. 155 et s. ; B. HAVELANGE et A.-C. LACOSTE, « Les flux transfrontaliers de données à caractère personnel en droit européen », *J.T. dr. eur.*, 2001, pp. 241 à 248. Cette interprétation a par ailleurs été confirmée par le Groupe de l'article 29 (*WP* 37, « Le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne », document de travail adopté le 21 novembre 2000, pp. 30 et 31, disponible à http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37fr.pdf) et par la Commission de protection de la vie privée (avis 34/2000 du 22 novembre 2000 relatif à la protection de la vie privée dans le commerce électronique, p. 8).

gique. Une protection adéquate des données envoyées à l'étranger en provenance de Belgique est exigée.

La réponse contenue à l'article 3*bis* vise à couvrir, quant à elle, les situations dans lesquelles les sujets des données se voient privés, par une manœuvre artificielle, du bénéfice de la protection de l'ensemble de la loi, et les situations échappant à toute protection, même celle instaurée en matière de flux transfrontières. Dans ce sens, deux catégories de situations entrent, selon nous, dans le champ de l'article 3*bis* :

- celle précisément où un *responsable de traitement cherche délibérément à contourner la loi* et, pour ce faire, délocalise son établissement vers un pays tiers à l'Union européenne, tout en faisant usage de moyens localisés sur le territoire belge pour réaliser son traitement ;
- celle où le flux est le fait exclusif d'un responsable localisé dans un pays tiers. Il s'agit des *flux de données passifs*, c'est-à-dire ceux qui se font à l'insu de la personne concernée et pour lesquels c'est l'utilisation à distance de l'équipement de l'internaute qui déclenche la collecte de données.
  C'est le cas d'une collecte de données effectuée par le biais de *cookies*, à l'insu de la personne concernée, au sein même de son ordinateur[1]. Les *cookies* auront été discrètement déposés par le responsable d'un site Internet sur le disque dur du « surfeur » belge, à l'occasion d'une de ses visites du site en question. Les dispositions concernant les flux transfrontières de données ne trouvent pas à s'appliquer à cette hypothèse[2]. Pour combler le vide de protection, l'article 3*bis* a alors toute sa pertinence. C'est donc le régime complet de la directive qui va s'appliquer au traitement de données obtenues à l'aide de *cookies*, et non le régime spécifique – plus souple – des flux transfrontières.
  Le cas de la collecte de données via des voitures sillonnant les rues du pays pour établir par la suite un service de géolocalisation (du type de Google StreetView) illustre aussi la situation de « recours à des moyens localisés sur le territoire belge, dans le but de traiter des données à caractère personnel ». Il est clair que les personnes concernées par les données collectées lors du passage de ce type de voitures n'effectuent pas un flux transfrontière de données au moment de l'enregistrement des images et des points d'accès Wi-Fi par les capteurs de la voiture. Ce traitement de données doit tout de même être couvert par les règles de protection. Ce sera le cas soit si le responsable du service de géolocalisation en question est établi sur le territoire belge ou européen, soit, si ce n'est pas le cas, du fait du recours aux véhicules munis de capteurs enregistreurs, sur le territoire belge.

1. Entre de la même manière, dans cette hypothèse, l'envoi de bannières en JavaScript ou de puces permettant d'identifier l'équipement utilisé par le « surfeur » comme le Global Unique Identifier.
2. Voy. l'explication détaillée donnée *in* M.-H. BOULANGER et C. DE TERWANGNE, *op. cit.*, p. 203.

Dans ces deux hypothèses, le critère déterminant de l'application de la loi belge aux responsables établis hors de l'Union européenne ne se réduit pas à l'utilisation de moyens situés sur le territoire du pays. Cette utilisation n'est qu'un élément de l'analyse du contexte des opérations effectuées. Une analyse plus globale s'impose en effet pour pouvoir constater, le cas échéant, que le responsable du traitement est anormalement établi à l'étranger alors que son activité est orientée sur la Belgique ou que l'on se trouve en présence d'une situation échappant à toute protection, notamment à celle issue du régime des flux transfrontières.

5. Les principes fondamentaux de la loi

Pour être admissibles aux yeux de la loi de 1992, les traitements de données opérés doivent répondre à plusieurs conditions. Ces conditions tiennent, d'une part, aux traitements eux-mêmes et, d'autre part, aux données traitées. Ainsi donc, pour être licite, un traitement de données à caractère personnel doit être loyal et transparent, doit poursuivre une finalité déterminée, explicite et légitime (principe de finalité)[1] et s'identifier à une des hypothèses reprises dans la liste de l'article 5 de la loi de 1992 (principe de proportionnalité). En outre, seules les données respectant les principes de finalité et de proportionnalité peuvent faire l'objet du traitement. Les données doivent, en outre, présenter des qualités d'exactitude et de mise à jour.

Le non-respect de chacune des conditions mentionnées ci-dessus et présentées dans les pages qui suivent est punissable pénalement : d'une amende et/ou d'un emprisonnement en cas de récidive.

Avant d'exposer ces principes clés du régime de protection mis en place, il convient de signaler qu'un certain ordre peut utilement être suivi lors de la vérification du respect de ces principes dans le cas d'un traitement de données considéré. Pour être plus aisées, la lecture de la loi et son application à un cas concret peuvent suivre le schéma suivant (chacune des étapes de ce schéma étant expliquée et développée dans les points qui suivent) :

- vérifier si les données à caractère personnel sont traitées loyalement et licitement ;
- vérifier si les finalités du traitement sont déterminées, explicites et légitimes ;
- pour ce dernier point, appliquer l'article 5 de la LVP en cas de données à caractère personnel ordinaires et les articles 6 à 8 en présence de données sensi-

1. Article 4, § 1er, 2°, de la loi du 8 décembre 1992.

bles, pour vérifier si le traitement correspond à l'une des bases de légitimité listées dans ces dispositions ; revenir à l'article 4 pour vérifier concrètement si la finalité du traitement ne viole pas le principe de proportionnalité ;
- cette étape accomplie, vérifier si les données sont bien pertinentes, adéquates et non excessives au regard des finalités poursuivies.

5.1. La protection du droit au respect de la vie privée et des autres libertés lors du traitement de données à caractère personnel

L'article 2 de la LVP énonce que, « [l]ors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée ».

La loi vise à la protection de l'ensemble des libertés et droits fondamentaux des individus, parmi lesquels leur droit à la vie privée, en présence de traitements de données à caractère personnel[1]. Ainsi qu'on l'a déjà signalé à l'entame de ce chapitre, l'objet de la loi n'est, en effet, pas limité à la protection de la seule vie privée.

Il est vrai que la protection des données à caractère personnel met en cause la protection d'autres droits et libertés que le droit au respect de la vie privée, tels la liberté de se déplacer (traitement de données de géolocalisation), la liberté d'association (fichiers des membres de groupes et d'associations), la liberté de s'informer et de s'exprimer en toute transparence (ne pas voir les informations filtrées en fonction de profils préétablis), le droit de pétition, de se loger, de trouver un emploi, le droit à la non-discrimination, etc.

> « Ainsi, pour parler de la liberté d'expression et de la liberté d'association, comment imaginer que celles-ci puissent survivre si la personne se sait surveillée dans ses communications et ne peut à certains moments s'exprimer anonymement si la technologie garde systématiquement trace de ses messages ? La liberté de s'informer suppose que l'information ne soit pas filtrée, que l'on ne soit pas conduit, profilage aidant, à son insu ou malgré soi, vers l'information qu'autrui souhaite nous voir consommer. Pire, la même technique de profilage peut amener l'auteur du profilage à priver de certains services ou informations un consommateur pour lequel il estime qu'il est peu rentable de l'autoriser à y avoir accès »[2].

1. Voy. Y. POULLET, « La protection des données : entre libertés, droits subjectifs et intérêts légitimes », *in Liber amicorum Paul Martens*, Bruxelles, Larcier, 2007, pp. 133 à 150.
2. Y. POULLET, J.-M. DINANT, C. DE TERWANGNE et M.-V. PEREZ-ASINARI, *L'autodétermination informationnelle à l'ère de l'Internet*, Rapport pour le Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), Conseil de l'Europe, Strasbourg, 18 novembre 2004.

5.2. Les principes de loyauté et de licéité

Aux termes de l'article 4, § 1er, 1°, les données à caractère personnel doivent être traitées loyalement et licitement.

5.2.1. L'exigence de loyauté

L'exigence de loyauté induit que le traitement des données soit réalisé dans la transparence pour les personnes concernées, et sans tromperie. Les traitements de données ne peuvent se faire à l'insu des personnes sur qui portent les données.

Le principe de loyauté est donc lié au devoir de transparence qui sera exposé dans des développements ultérieurs, au point 7.1.2. Ce devoir de transparence implique que certaines informations soient fournies spontanément par le responsable du traitement aux personnes concernées. L'obligation de fournir des informations est à géométrie variable, liée précisément à l'exigence de loyauté : au-delà de certains renseignements à donner en toutes circonstances, d'autres informations ne sont à transmettre que si cela est nécessaire pour garantir la loyauté du traitement des données. Ces informations supplémentaires portent sur les destinataires des données traitées, le fait que les données seront transmises au-delà des frontières, etc. L'idée, on le voit, est d'annoncer loyalement aux personnes concernées le sort qui attend leurs données.

La loyauté du traitement de données ne se limite pas à la collecte, mais doit être garantie à toutes les étapes de celui-ci.

Le cas tranché par le Tribunal correctionnel de Bruxelles[1] dans une affaire dans laquelle l'ASBL Gaïa était impliquée illustre cette question de loyauté. C'est au niveau de la collecte des données que la loyauté a fait défaut dans ce cas. Dans ce dossier, la preuve rapportée était entièrement fondée sur une vidéo prise au moyen d'une caméra cachée. Cette pratique dans la récolte de preuves fut jugée comme plaçant la défense dans l'impossibilité de vérifier l'authenticité et l'exhaustivité des images. De sorte que la preuve a été déclarée non recevable.

5.2.2. Préférence pour une collecte directe auprès de la personne concernée[2]

Dans certaines circonstances, le devoir de loyauté implique que préférence soit donnée à la collecte de données directement auprès des personnes concernées, et non pas de manière indirecte auprès de sources tierces.

1. Corr. Bruxelles (51e ch.), 14 janvier 2002, *A.M.*, 2002, pp. 197 à 199.
2. V. VERBRUGGEN, *Les Codes commentés. La protection des données*, Bruxelles, Larcier, 2011, pp. 55 et 56.

C'est le cas dans un contexte d'emploi, notamment lors des procédures de recrutement des employés[1].

En présence de données médicales, le principe édicté par la Recommandation n° R(97)5 du Comité des ministres du Conseil de l'Europe relative aux données médicales[2] consiste en ce que « les données médicales doivent en principe être collectées *auprès de la personne concernée*. Elles ne peuvent être collectées auprès d'autres sources que conformément aux principes 4, 6 et 7 de la présente recommandation, et à condition que cela soit nécessaire pour réaliser la finalité du traitement ou que la personne concernée ne soit pas en mesure de fournir les données »[3].

5.2.3. La loyauté en présence d'un enfant

Les autorités européennes en charge du contrôle du respect de la législation de protection des données[4] ont insisté sur le fait que « l'obligation de traiter les données à caractère personnel conformément au principe de loyauté (article 6, point a) doit être interprétée strictement lorsqu'un enfant est concerné. Dans la mesure où un enfant n'est pas encore complètement mûr, les responsables du traitement doivent en avoir conscience et agir en toute bonne foi lors du traitement de ses données »[5].

5.2.4. L'exigence de licéité

Quant à l'exigence de traiter licitement les données, elle signifie que le traitement de données à caractère personnel doit se faire conformément à l'ensemble des règles légales. Cela inclut les règles contenues dans la loi vie privée elle-même, mais également toute autre règle qui trouverait à s'appliquer à une situation de traitement de données. Ainsi, la règle du secret professionnel doit être respectée en sus de la loi du 8 décembre 1992 lorsque des opérations sont appliquées à des données médicales à caractère personnel.

5.3. Le principe de finalité

Principe clé de la protection, le principe de finalité exige que tout traitement poursuive une ou des finalité(s) déterminée(s), explicite(s) et légitime(s), que l'on ne fasse que ce qui est compatible avec cette (ces) finalité(s), que l'on ne traite que les données perti-

1. Recommandation n° R(89)2 du Comité des ministres du Conseil de l'Europe sur la protection des données à caractère personnel utilisées à des fins d'emploi, 1989, point 4.
2. Au point 4.2.
3. V. VERBRUGGEN, *Les Codes commentés. La protection des données*, *op. cit.*, p. 55.
4. Groupe de l'article 29, avis 2/2009 du 11 février 2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles), *WP* 160. Voy. également Groupe de l'article 29, document de travail 1/2008 du 18 février 2008 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles), *WP* 147.
5. V. VERBRUGGEN, *Les Codes commentés. La protection des données*, *op. cit.*, p. 56.

nentes au vu de la (des) finalité(s) et que l'on ne conserve ces données qu'aussi longtemps que cela est nécessaire pour atteindre la finalité du traitement.

Ce principe repose sur le postulat que « le danger inhérent aux traitements de données à caractère personnel réside davantage dans les finalités qu'ils poursuivent que dans la nature des données qui en font l'objet »[1].

5.3.1. Finalité du traitement déterminée, explicite et légitime

L'article 4, § 1er, 2°, de la LVP prescrit que les données à caractère personnel « doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables ».

La finalité d'un traitement de données signifie la raison pour laquelle le traitement est effectué[2].

a) Finalité déterminée

Tout traitement de données doit poursuivre une ou des finalité(s) déterminée(s). Il s'agit de savoir, dès le démarrage d'un traitement de données, quel(s) objectif(s) ce traitement est appelé à servir. La finalité ne peut être inexistante (« on ne sait pas encore à quoi vont servir ces données mais comme on a l'occasion de les collecter, collectons-les toujours ») ni floue.

La spécification de la finalité est fondamentale, car c'est elle qui va déterminer le traitement de données à caractère personnel et permettre à la personne concernée de contrôler le sort réservé aux données la concernant. « La finalité se présente en effet comme le critère central de la vérification du respect de la protection instaurée : tant le contrôle de la légitimité de la finalité que celui de la conformité des données traitées à cette dernière suppose[nt] que ladite finalité soit connue »[3].

La finalité doit être précise afin de permettre à la personne concernée d'effectuer cette analyse et d'exercer les droits qui lui sont conférés par la loi. Cette précision permettra également au responsable du traitement de déterminer les données qui devront être collectées et traitées. En effet, comme on le verra plus loin, les données traitées doivent être pertinentes au regard de la finalité. Une finalité qui ne serait pas

1. Voy. M.-H. Boulanger, C. de Terwangne et Th. Léonard, « La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel », *J.T.*, 1993, p. 377.
2. P. De Hert et D. Pissoort, *in Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2004, p. 85.
3. M. Van Overstraeten et S. Depré, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, pp. 685 et 686. Voy. aussi M.-H. Boulanger, C. de Terwangne et Th. Léonard, *op. cit.*, p. 377.

suffisamment précise et serait donc énoncée de manière trop large permettrait de traiter un ensemble bien trop vaste de données, toutes pouvant passer pour pertinentes par rapport à la finalité annoncée.

Le Groupe 29 a affirmé expressément que les finalités d'un traitement de données doivent être définies avec précision. Il l'a fait notamment dans son avis portant sur les traitements de données effectués par les agences antidopage : « La simple référence au traitement des données par les organisations antidopage "dans le contexte de leurs activités antidopage" et une formule du type "les organisations antidopage ne doivent traiter les renseignements personnels que dans la mesure nécessaire et appropriée pour assumer les responsabilités qui leur incombent en vertu du code et des standards internationaux" ne suffisent pas »[1].

On peut trouver, dans la liste des finalités proposée sur son site par la Commission de la protection de la vie privée afin d'aider les responsables de traitement à effectuer la formalité de déclaration (voy., *infra*, le point 7.1.1. réservé à cette formalité), des modèles de finalités déterminées avec suffisamment de précision. On trouve, par exemple, dans cette liste « administration du personnel », « contrôle sur le lieu de travail », « lutte contre la fraude et les infractions de la clientèle », « collecte de dons », « relations publiques », « gestion du contentieux », « gestion de bibliothèque », « octroi de crédit », « service de courtage », etc.

Déterminer la finalité poursuivie par le traitement de données à caractère personnel se révèle donc une étape essentielle en matière de protection des données à caractère personnel.

Il est à noter que cette finalité doit être reprise dans la déclaration de traitement afin d'également permettre à la Commission de la protection de la vie privée d'effectuer un contrôle.

b) Finalité explicite

La finalité doit également être explicite, ce qui signifie qu'elle doit être annoncée, ne pas être tenue « secrète » ou « camouflée »[2].

Comme on le verra ultérieurement au point 7.1., la transparence des traitements de données fait partie intégrante du régime de protection. La ou les finalités du traitement entrepris sont parmi les éléments les plus importants à communiquer au nom

1. Groupe de l'article 29, deuxième avis 4/2009 du 6 février 2009, sur le standard international pour la protection des renseignements personnels de l'Agence mondiale antidopage (AMA), sur les dispositions du code de l'AMA s'y rapportant et sur d'autres questions relatives à la vie privée dans le cadre de la lutte contre le dopage dans le sport par l'AMA et les organisations (nationales) antidopage (*WP* 162).
2. C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *Cabinet d'avocats et technologies de l'information : balises et enjeux*, coll. Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005, p. 157.

de l'obligation de transparence. L'information sur la finalité poursuivie doit être systématiquement dévoilée lors de la mise en œuvre de tout traitement.

c) Finalité légitime

Enfin, la finalité doit être légitime, ce qui signifie que la finalité ne peut induire une atteinte disproportionnée aux droits, libertés et intérêts en jeu, au nom des intérêts poursuivis par le responsable du traitement[1]. « La notion de légitimité invite donc à un examen de proportionnalité. On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées »[2].

Les intérêts en jeu à prendre en considération sont, bien sûr, ceux de la personne concernée par les données, mais sont aussi, le cas échéant, l'intérêt de la société dans son ensemble. Une recherche médicale, par exemple, met en jeu l'intérêt des malades auprès de qui on a recueilli les données relatives à leur santé, intérêt à voir garantir la confidentialité de ces données, l'intérêt de l'équipe de chercheurs désireux de faire avancer l'état des connaissances scientifiques, mais également l'intérêt de la société, du point de vue de la santé publique, à voir progresser les possibilités de traitement de la maladie étudiée.

En résumé, pour être légitime, une finalité ne peut causer un préjudice plus grand à l'ensemble des intérêts en jeu que l'intérêt que représente le traitement.

Dans le même sens d'ailleurs, dans le cadre de l'article 8 CEDH, la jurisprudence de la Cour européenne des droits de l'homme exige un juste équilibre entre les intérêts publics et privés en jeu lors de la mise en œuvre de traitements de données. Dans son arrêt *S. et Marper*[3], la Cour a ainsi affirmé que le traitement de données doit être proportionné, c'est-à-dire approprié par rapport aux buts légitimes poursuivis, nécessaire dans la mesure où il n'existe pas d'autres mesures appropriées moins attentatoires aux intérêts, droits et libertés des personnes concernées ou de la société, et qu'il ne peut induire une atteinte démesurée à ces intérêts, droits et libertés par rapport aux bénéfices attendus par le responsable du traitement.

---

1. M.-H. Boulanger, C. de Terwangne et Th. Léonard, « La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel », *J.T.*, 1993, pp. 377 et 379 ; M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreaux et Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p. 145 ; J. Dumortier et F. Robben, note sous Prés. Comm. Anvers, 7 juillet 1994, et Prés. Comm. Bruxelles, 15 septembre 1994, *Computerr.*, 1994, pp. 244 et s ; S. Gutwirth, « De toepassing van het finaliteitbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens », *T.P.R.*, 1993/4, pp. 1409 et s. ; Th. Léonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », *in* F. Rigaux, *La vie privée, une liberté parmi les autres ?*, Travaux de la Faculté de droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s.
2. C. de Terwangne, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *op. cit.*, p. 157.
3. Cour eur. D.H. (Gr. Ch.), arrêt S. et Marper c. Royaume-Uni, 4 décembre 2008, req. n^{os} 30562/04 et 30566/04, § 118.

Les décisions de jurisprudence reprises ci-dessous illustrent des hypothèses où un traitement de données a été jugé comme causant une atteinte disproportionnée aux droits et intérêts des personnes concernées.

La Cour d'appel de Gand[1] a été saisie d'une affaire dans laquelle la preuve d'un vol était apportée au moyen d'images issues d'une vidéo réalisée par une caméra de surveillance visible, accrochée sur la façade extérieure d'un bâtiment de la Banque nationale. Étaient filmées les personnes se trouvant sur le trottoir devant la Banque nationale. Celle-ci ne procédait cependant pas à leur identification systématique. La banque réalisait ces prises de vues afin de prévenir et d'établir les atteintes à sa sécurité et la Cour a relevé qu'il n'était démontré d'aucune manière crédible que les images étaient utilisées pour d'autres finalités. La Cour d'appel estima que la licéité du traitement devait être jugée en application du principe de proportionnalité : l'intérêt général ou les intérêts légitimes du responsable de traitement doivent primer le droit à la protection de la vie privée de la personne concernée, ce qui implique que la menace accessoire pour la vie privée provenant de la prise d'images doit être compensée par une valeur ajoutée décisive que l'enregistrement offre dans l'accomplissement de l'objectif qu'il poursuit. Dans le cas d'espèce, la Cour a pris en compte dans son analyse le droit à la sûreté (art. 5 CEDH), le droit à l'inviolabilité du domicile (art. 8 CEDH), le droit de propriété (art. 544 C. civ.), la loi du 10 avril 1990 réglementant la sécurité privée et particulière et, enfin, l'article 5, f), de la LVP. Elle a jugé que, dans le cas d'espèce, l'intérêt ou les droits fondamentaux de la personne concernée ne pesaient pas plus lourd et que l'utilisation des images prises par les caméras en cause ne devait pas être limitée aux infractions dont la banque était victime en tant que telle.

Une autre affaire mettait en cause la diffusion des informations commerciales de la banque de données « Creditel ». Parmi les informations à fournir au sujet d'une société figuraient les mandats antérieurs exercés par ses administrateurs. Le Tribunal de commerce de Courtrai fut appelé à se prononcer sur la légitimité de ce traitement de diffusion de données. Pour effectuer la mise en balance des intérêts en présence, le Tribunal a pris en compte, d'une part, la pertinence de l'information pour celui qui la traite et, d'autre part, la nature de cette information. D'après le tribunal, le caractère public des données doit également être pris en compte dans la réalisation de cette mise en balance. Le traitement fut considéré comme légitime[2].

La Cour constitutionnelle s'est prononcée[3] dans un cas où, d'après un décret flamand, les suspensions disciplinaires des sportifs majeurs devaient être publiées pour leur durée sur un site Web créé par le gouvernement à cette fin et via les canaux de

1. Gand, 28 mars 2002, *T. Strafr.*, 2002, pp. 326 à 334.
2. Comm. Courtrai (1ᵉ ch.) 19 juin 2003, *T.G.R.-T.W.V.R.*, 2007, liv. 2, p. 100, confirmé par Gent, 6 januari 2005, *T.G.R.-T.W.V.R.*, liv. 2, 2007, pp. 92 et 93.
3. C.A., 20 octobre 2004, n° 162/2004, suspension, point B.5.2 ; puis C.A., 19 janvier 2005, n° 16/2005, annulation http://www.const-court.be, point B.1.

communication officiels créés par les fédérations sportives. Cette publication contenait les nom, prénom et date de naissance du sportif, le début et la fin de la période de suspension et la discipline sportive qui avait donné lieu à l'infraction. La Cour a limité son examen à la publication sur le site Web créé par le gouvernement ; il s'agit d'une ingérence dans le droit au respect de la vie privée. Assurer le respect effectif des sanctions imposées aux sportifs est un but légitime, mais « [l]a diffusion de données personnelles, prévue par le décret, sur un site Web non sécurisé et, partant, accessible à chacun va cependant au-delà de ce que cet objectif requiert ». La Cour conclut que « la publication entreprise n'est pas nécessaire pour atteindre l'objectif légitime poursuivi par le législateur décrétal, puisque cet objectif peut également être réalisé d'une manière moins dommageable pour les intéressés et, d'autre part, les effets de la mesure sont disproportionnés par rapport à cet objectif ».

5.3.2. Utilisations compatibles

a) La règle

Après avoir spécifié que les données à caractère personnel doivent être collectées pour une ou plusieurs finalités déterminées, explicites et légitimes, la loi dispose que les données ne peuvent pas « être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables »[1].

Une fois qu'on a collecté des données à caractère personnel, on ne peut en faire n'importe quoi. Seules les utilisations compatibles avec la ou les finalités déterminées et annoncées au départ, au moment de la collecte, sont admises.

b) Le critère des prévisions raisonnables

Pour savoir si une utilisation est compatible avec la finalité de collecte des données, il faut tenir compte notamment des prévisions raisonnables des personnes concernées. Si l'utilisation envisagée offre un lien logique avec la finalité annoncée, les personnes concernées peuvent raisonnablement s'attendre à ce qu'une telle utilisation ait lieu. Elle sera donc jugée compatible et sera, dès lors, légale.

Ce critère des prévisions raisonnables est tout à fait pertinent, car la loi a pour but, ainsi qu'exposé plus haut au point 2.2.1. traitant de l'objet de la loi ainsi que dans l'introduction du présent ouvrage, de garantir la maîtrise par les individus du sort réservé aux données les concernant. On a précisé que, par la « maîtrise », on entend notamment le fait de connaître le sort qui est réservé à ses données. Maintenir tout ce qui est fait avec les données dans les prévisions des personnes concernées est la

1. Article 4, § 1er, 2°, LVP.

meilleure façon de permettre à chacun de conserver le contrôle sur le sort de ses données.

La loi propose également comme critère de compatibilité le fait que le traitement soit prévu par des dispositions légales ou réglementaires. Il est impératif que les dispositions en question répondent aux exigences de l'article 8, § 2, CEDH[1]. Pour être retenues comme légitimant des opérations effectuées sur des données, les dispositions légales ou réglementaires doivent être accessibles et surtout prévisibles, selon le prescrit de l'article 8, § 2. L'exigence de prévisibilité impose que la norme soit rédigée avec suffisamment de précision. À sa lecture, les personnes concernées doivent comprendre qu'un traitement sera opéré sur des données les concernant qui avaient été collectées dans un but initial différent de celui poursuivi par ce traitement ultérieur.

c) Exemples d'incompatibilité et de compatibilité

À titre d'exemple d'utilisations des données qui ne sont pas compatibles, on citera :

- le cas d'un club de sport qui céderait la liste de ses adhérents avec toutes leurs coordonnées à une entreprise vendant des produits de régime amincissant afin de permettre à cette entreprise de contacter les membres du club pour leur proposer ses produits ;
- les cas traités par la Commission de la protection de la vie privée concernant un bourgmestre ayant utilisé le fichier des parents d'un enfant inscrit dans la crèche communale pour leur envoyer un courrier électoral pour les élections auxquelles il se représentait, un autre bourgmestre utilisant le registre des mariages pour envoyer ses vœux aux mariés de l'année en les invitant à se souvenir de lui dans les isoloirs et, encore, un autre bourgmestre utilisant le fichier des patients de l'hôpital établi dans sa commune pour leur souhaiter en son nom propre un prompt rétablissement ;
- le cas d'une banque ayant également des activités d'assurance, qui identifie dans les virements effectués par ses clients ceux qui paient des primes d'assurance plus élevées que les primes de ses produits d'assurance et qui leur envoie un courrier les invitant sur cette base à changer de compagnie d'assurances[2] ;
- le cas d'un médecin qui utilise les données d'un patient soigné par lui pour alimenter la recherche d'un laboratoire pharmaceutique ou même ses propres recherches ;
- le cas d'un établissement scolaire qui communique les informations sur ses élèves en difficulté à des sociétés proposant un soutien scolaire[3].

---

1. Voy. la partie du présent ouvrage consacrée à l'article 8 CEDH.
2. Anvers, 3 mai 1999, *Ann. prat. comm.*, 1999, pp. 524 à 527 ; *A.J.T.*, 1999, p. 437, note C. De Vos ; appel de Prés. Comm. Anvers, 7 juillet 1994, *D.C.C.R.*, 1994-1995, p. 77, note Th. Léonard.
3. Pour d'autres exemples encore, voy. B. Docquir, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, pp. 128 et 129.

Dans certains des cas cités ci-dessus, les utilisations mentionnées pourraient être effectuées, mais elles seraient considérées comme déclenchant un nouveau traitement de données, devant dès lors répondre aux exigences inhérentes à un nouveau traitement, telless que l'information des personnes concernées à propos de la nouvelle perspective d'utilisation de leurs données et le respect d'une des hypothèses de légitimation des traitements énoncées à l'article 5 (voy. *infra*).

Ainsi, le club de sport pourrait communiquer les données de ses adhérents, mais seulement en informant ceux-ci auparavant et en récoltant leur consentement pour ce faire. Il en serait de même pour le médecin désireux de réutiliser les données contenues dans les dossiers de ses patients à des fins de recherche[1] à moins que ce soit dans le cadre des activités, par exemple, d'un CHU qui serait couvert par ses missions légales de recherche[2]. L'école, quant à elle, ne pourrait certes en aucun cas communiquer les données en question à des fins commerciales, mais pourrait, si cela entre dans sa politique de communication interne, appliquer la voie moins attentatoire consistant à faire circuler la publicité au sein de l'établissement.

Un cas fréquent concernant la profession d'avocat mérite d'être évoqué ici : « La pratique développée dans les barreaux de recourir à la sous-traitance pour l'ensemble ou une partie d'un dossier ne pourra être considérée comme compatible avec la finalité de gestion du dossier confié à l'avocat initial que si le client concerné a connaissance d'une telle démarche et de l'identité du sous-traitant. Cela est d'autant plus vrai que la relation liant un client à l'avocat qu'il choisit est une relation *intuitu personae* marquée par la confiance[3]. Par contre, rien n'empêche un avocat de consulter un confrère spécialisé dans un domaine juridique particulier dès lors qu'il ne communique pas les éléments permettant d'identifier le client en cause. Il ne sera bien évidemment pas tenu d'en informer le client »[4].

d) La communication de données

On ne peut communiquer les données à caractère personnel que l'on traite à n'importe qui ni pour n'importe quel motif[5]. Toute communication de données doit respecter le principe de finalité. Cela implique que l'on ne peut communiquer les

1. Voy. Recommandation n° R (97) 5 du Comité des ministres du Conseil de l'Europe sur la protection des données médicales, 1997 (point 12 « Recherche scientifique ») : 12.3 – « Sous réserve de conditions complémentaires prévues par le droit interne, les professionnels des soins de santé habilités à mener leurs propres recherches médicales devraient pouvoir utiliser les données médicales qu'ils détiennent pour autant que la personne concernée ait été informée de cette faculté et ne s'y soit pas opposée. »
2. Voir J. Herveg, «La Réglementation des traitements de données à caractère personnel concernant le patient dans les hôpitaux », in *Guide hospitalier*, Kluwer, 2009, 10.1.
3. De toute manière, un devoir d'information impose d'indiquer à la personne concernée les destinataires de ses données. Voy. *infra*.
4. C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *in Cabinet d'avocats et technologies de l'information : balises et enjeux*, coll. Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005, p. 158.
5. Voy. les amples développements réservés à la communication.

données qu'aux personnes et que dans les cas qui découlent des finalités de collecte des données ou qui sont compatibles avec ces finalités.

C'est donc en tenant compte de la finalité initiale du traitement de données que l'on saura à qui on peut transmettre les données. Toute opération de mise à disposition des données devra se faire de manière compatible avec cette finalité initiale. Des données collectées à des fins de gestion administrative par une autorité publique ou un établissement scolaire, par exemple, ne peuvent être communiquées à qui que ce soit à des fins commerciales. De telles fins ne peuvent passer pour compatibles avec une finalité initiale d'intérêt public, induisant, en outre, une collecte obligatoire des données.

La Cour de justice de l'Union européenne a eu l'occasion, dans l'affaire *Deutsche Telekom*, de se prononcer sur la compatibilité du transfert des coordonnées téléphoniques des abonnés par l'opérateur à d'autres prestataires désireux d'éditer des annuaires téléphoniques. Cette affaire se place dans le contexte de l'article 12, § 2, de la directive 2002/58 exigeant le consentement des abonnés à des services de télécommunications pour la publication des données à caractère personnel les concernant dans les annuaires publics[1]. « La Cour a déterminé qu'"*il ressort d'une interprétation contextuelle et systématique de l'article 12 que le consentement porte sur la finalité de la publication des données à caractère personnel dans un annuaire public et non sur l'identité d'un fournisseur d'annuaire en particulier*"[2]. Dès lors, le consentement dûment informé des abonnés à la publication des données le concernant dans un annuaire public "*s'étend ainsi à tout traitement ultérieur desdites données par des entreprises tierces actives sur le marché des services de renseignements téléphoniques accessibles au public et d'annuaire, pour autant que de tels traitements poursuivent cette même finalité*"[3]. La transmission des données en question entre entreprises aux fins de publication d'annuaires publics ne requiert pas l'obtention d'un nouveau consentement de la part des abonnés et ne porte pas atteinte à la substance même du droit à la protection des données à caractère personnel tel que reconnu à l'article 8 de la Charte[4] »[5].

1. C.J.U.E., 5 mai 2011 (Deutsche Telekom a.g. c. Allemagne), aff. C-543/09.
2. *Idem*, point 61.
3. *Idem*, point 65.
4. *Idem*, point 66.
5. C. GAYREL, « Chronique de jurisprudence en droit des technologies de l'information (2009-2011). Libertés et société de l'information. Cour de Justice de l'Union européenne, Tribunal de Première Instance et Tribunal de la Fonction publique européenne », *R.D.T.I.*, n^os 48 et 49, 2012, p. 112.

5.3.3. Traitements ultérieurs à des fins historiques, scientifiques et statistiques[1]

La loi vie privée prévoit, en son article 4, 2°, qu'« un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par le Roi, après avis de la Commission de la protection de la vie privée ». Cette présomption de compatibilité implique donc que le traitement ultérieur à des fins historiques, statistiques ou scientifiques soit conforme aux conditions fixées par le Roi en vertu de son habilitation ; conditions qui figurent dans l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et, plus particulièrement, à son chapitre II relatif au traitement ultérieur à caractère personnel à des fins historiques, statistiques ou scientifiques[2].

Le système prévu par l'arrêté royal doit se voir comme une application du principe de proportionnalité vu par ailleurs au point 5.3.1, c). En effet, il établit un principe de « cascade » – ou « une réglementation en trois stades »[3] – consistant à privilégier les données sous une forme qui permet de ne pas identifier – ou le moins possible – la personne concernée. Ainsi, les données anonymes seront privilégiées par rapport à tout autre type de données[4]. Il s'agit d'un principe de base institué par l'arrêté royal[5].

Si le traitement ultérieur à des fins historiques, statistiques ou scientifiques ne peut être mené avec de telles données, alors seulement des données codées peuvent être utilisées et, si cette forme ne permet pas non plus d'effectuer le traitement, les données non codées peuvent être utilisées.

Nous constatons donc que les données non codées ne peuvent être utilisées qu'en tout dernier ressort.

Chacune des trois possibilités répond à des règles différentes.

---

1. Voy. également C. DE TERWANGNE et S. LOUVEAUX, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.*, 2001, pp. 457 à 469.
2. Sur cette question, voy. J. VANDENDRIESSCHE, « De verwerking van persoonsgegevens voor historische, statistische en wetenschappelijke doeleinden », *T.B.B.R.-R.G.D.C.*, 2006, pp. 534 à 543 ; D. DE BOT, *Verwerking van persoonsgegevens*, Antwerpen, Kluwer, 2001, pp. 132 et s. ; L. DEPLANQUE et N. VERHAEGHEN, « La réutilisation de données à caractère personnel relatives à la santé en recherche médicale sous l'angle du droit belge », *T. Gez.*, 2004-2005, pp. 24 et s.
3. Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001, p. 7848.
4. Article 3 de l'arrêté royal du 13 février 2001.
5. Rapport au Roi précédant l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001, p. 7848.

a) Données anonymes

Par « données anonymes », l'on entend « les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont donc pas des données à caractère personnel ». Cela signifie que le lien entre la personne concernée et la donnée le concernant doit être rompu. Qui dit donnée anonyme dit également que le traitement de telles données ne tombe pas dans le champ d'application de la loi vie privée (voy. *supra*).

Nous devons attirer l'attention sur le fait que, si certaines données paraissent anonymes *prima facie*, mises ensemble, il se peut qu'elles permettent d'identifier la personne concernée. Nous pouvons illustrer ce propos par un exemple en matière médicale. Imaginons un chercheur qui travaille sur les données concernant un patient dont le nom a été remplacé par un code qui ne permet pas de mettre la donnée en lien avec le patient, car la table de conversion a été détruite. Les données sont donc, au sens de l'arrêté royal, anonymes. Cependant, ce chercheur réussit – volontairement ou non – à accumuler différentes informations concernant ce patient tel que l'hôpital où il a été soigné, les jours d'hospitalisation, le service, son lieu de résidence et sa date de naissance. Si ces divers éléments pris isolément ne permettent pas une identification, ils le peuvent par leur mise en lien. On arriverait donc à une situation dans laquelle les données ne sont plus anonymes dès lors que, mises ensemble, elles peuvent être mises en relation avec une personne, à tout le moins, identifiable. De plus, l'évolution constante et de plus en plus rapide de la technologie (croisement de données, rapidité de calculs accrue, etc.) peut constamment mettre en péril l'anonymat de la donnée.

Il est donc clair que le caractère anonyme de la donnée devra être contrôlé de manière régulière afin de s'assurer de son effectivité. Il appartiendra au juge qui serait éventuellement saisi d'un cas d'espèce de s'assurer de cette effectivité.

La loi n'impose aucune condition particulière pour anonymiser les données hormis celle, à charge du responsable du traitement ultérieur à des fins historiques, statistiques ou scientifiques, de n'entreprendre aucune action pour convertir les données anonymes en données à caractère personnel codées ou pas[1]. Il est à noter que cette obligation vaut également pour les données codées.

b) Données codées

La section II de l'arrêté royal est relative au traitement ultérieur à des fins historiques, statistiques ou scientifiques utilisant des données codées qui sont, pour rappel, des

1. Article 6 de l'arrêté royal.

données à caractère personnel (voy. *supra*), et part du postulat que les données aient été « collectées pour des finalités déterminées, explicites et légitimes »[1].

Plusieurs hypothèses sont visées par le texte, chacune recevant une réponse légale différente.

La première hypothèse[2] prévoit que, si le traitement ultérieur à des fins historiques, statistiques ou scientifiques est effectué par ou pour le compte du responsable du traitement initial, les données doivent être codées, préalablement à ce traitement, soit par le responsable du traitement lui-même, soit par son sous-traitant s'il y est fait appel pour le traitement, soit encore par une organisation intermédiaire[3]. Si une telle organisation intermédiaire intervient dans le codage, ce sera pour le compte du responsable du traitement et donc comme sous-traitant au sens de l'article 1er, § 5, de la LVP.

La deuxième hypothèse est celle dans laquelle le responsable du traitement initial va transférer les données vers un tiers qui effectuera le traitement ultérieur à des fins historiques, statistiques ou scientifiques pour son propre compte. Dès lors qu'il y a un transfert de données à caractère personnel, le codage devra être effectué préalablement à ce transfert soit par le responsable du traitement initial, soit par une organisation intermédiaire qui sera le sous-traitant de ce dernier[4].

La troisième hypothèse recouvre le transfert de données à caractère personnel par plusieurs responsables de traitements initiaux à un même tiers en vue d'un traitement ultérieur à des fins historiques, statistiques ou scientifiques. Le codage des données à caractère personnel doit également être effectué préalablement au transfert, mais, à présent, par une organisation intermédiaire. Ce passage par une organisation intermédiaire s'explique par l'existence d'« une menace particulière pour la protection des données, dans la mesure où des données à caractère personnel provenant de différents transmetteurs de données sont rassemblées avant d'être codées »[5]. En corollaire à l'existence de ce risque, l'organisation intermédiaire sera elle-même un responsable du traitement[6] pour ce traitement précis qu'est la conversion de données à caractère personnel non codées en données codées.

L'arrêté royal prévoit également certaines conditions particulières à charge du responsable du traitement initial et/ou de l'organisation intermédiaire lorsque le traite-

1. Ce préalable est rappelé dans les articles 8, 9, 10, 12, 13, 14, 15 et 16 de l'arrêté royal.
2. Article 8 de l'arrêté royal.
3. Par « organisation intermédiaire », il faut entendre « la personne physique ou morale, l'association de fait ou l'administration publique, autre que le responsable du traitement des données non codées, qui code les données ».
4. Article 9 de l'arrêté royal.
5. C.P.V.P., avis n° 8/99, p. 3, et n° 25/99, p. 2.
6. Article 10 de l'arrêté royal.

ment ultérieur à des fins historiques, statistiques ou scientifiques implique un transfert de données :

- le transfert (hypothèses 1 et 2 ci-dessus) ne pourra s'opérer qu'après que le responsable de traitement ultérieur à des fins historiques, statistiques ou scientifiques aura présenté l'accusé de réception d'une déclaration complète, délivré par la Commission de la protection de la vie privée, conformément à l'article 17, § 2, de la LVP. Cela peut avoir un impact en termes de responsabilité dans le chef du responsable de traitement initial qui devra s'assurer que le responsable du traitement ultérieur possède effectivement cet accusé de réception, mais également que les données qui sont réclamées sont effectivement nécessaires audit traitement ultérieur. En effet, le transfert étant une partie du traitement dans le chef du responsable du traitement initial, il devra respecter les règles prévues par la loi, en ce compris celles portant sur la proportionnalité au niveau des données traitées. Il reste effectivement responsable de son traitement à tous les niveaux, en ce compris celui du transfert. La rédaction de l'article 13 prescrivant cette obligation de présentation de l'accusé de réception d'une déclaration pose question dès lors qu'il induit une différence de traitement – au sens des articles 10 et 11 de la Constitution – entre un responsable du traitement initial et un responsable du traitement ultérieur. En effet, un responsable du traitement initial peut bénéficier d'une exemption de déclaration en vertu de la section II de l'arrêté royal alors que celui d'un traitement ultérieur ne le pourrait pas dès lors qu'il est obligé de produire l'attestation de déclaration en vertu de l'article 13 de ce même Arrêté royal. Il y a manifestement discrimination entre responsables du traitement.
- préalablement au codage de données sensibles (art. 6 à 8 LVP) et uniquement de ces données, la personne concernée recevra les informations suivantes[1], à moins que « cette obligation se révèle impossible ou implique des efforts disproportionnés » ou « lorsque l'organisation intermédiaire est une autorité administrative chargée, explicitement par ou en vertu de la loi, de rassembler et de coder des données à caractère personnel et soumise, à cet égard, à des mesures spécifiques visant à protéger la vie privée, instituées par ou en vertu de la loi »[2] :
  - l'identité du responsable du traitement ;
  - les catégories de données à caractère personnel qui sont traitées ;
  - l'origine des données ;
  - une description précise des fins historiques, statistiques ou scientifiques du traitement ;
  - les destinataires ou les catégories de destinataires des données à caractère personnel ;

1. Article 14 de l'arrêté royal.
2. Article 15 de l'arrêté royal. Dans cette hypothèse, le responsable du traitement initial ou l'organisation intermédiaire doit le justifier auprès de la Commission de la protection de la vie privée dans le cadre de la déclaration visée par l'article 17 LVP. Un délai de quarante-cinq jours est alors ouvert pour permettre à la Commission de la protection de la vie privée de communiquer une recommandation assortie de conditions complémentaires.

- l'existence d'un droit d'accès aux données à caractère personnel qui la concernent et d'un droit de rectification de ces données ;
- l'existence d'un droit d'opposition de la personne concernée.

Pour en revenir à l'information devant être communiquée à la personne concernée visée par ce dernier point, si la lecture des commentaires d'articles peut laisser penser que l'information devrait être communiquée dans tous les cas[1], l'analyse de l'article 14 permet de considérer que cette obligation d'information n'est imposée que dans le cadre de traitements ultérieurs à des fins historiques, statistiques ou scientifiques qui portent sur des données visées aux articles 6 à 8 de la LVP. En effet, cette disposition précise que l'information doit être préalable au codage des données visées à ces articles 6 à 8 de la loi et se limite à ces seuls articles.

Il paraît donc légitime de s'en tenir aux termes de l'article 14 de l'arrêté royal et de considérer que l'obligation d'informations est limitée aux seules données sensibles.

c) Données non codées

L'arrêté royal met l'accent sur l'information de la personne concernée dès qu'il y a un traitement ultérieur à des fins historiques, statistiques ou scientifiques de données à caractère personnel non codées.

Ainsi, le responsable du traitement ultérieur à des fins historiques, statistiques ou scientifiques doit communiquer à la personne concernée un certain nombre d'informations dont son droit de consentir. Il peut être dérogé à cette obligation d'information ou de consentement lorsque[2] :

- le traitement ultérieur à des fins historiques, statistiques ou scientifiques se limite à des données à caractère personnel non codées, rendues manifestement publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou des faits dans lesquels celle-ci est ou a été impliquée ; ou
- ces obligations se révèlent impossibles ou requièrent des efforts disproportionnés et qu'il s'est conformé à la procédure déterminée à l'article 21 du présent arrêté.

---

1. Rapport au Roi précédant l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 13 mars 2001, pp. 7852 et s.
2. Dans cette hypothèse, le responsable du traitement ultérieur doit le justifier auprès de la Commission de la protection de la vie privée dans le cadre de la déclaration visée par l'article 17 LVP. Un délai de quarante-cinq jours est alors ouvert pour permettre à la Commission de la protection de la vie privée de communiquer une recommandation assortie de conditions complémentaires.

d) Publication des résultats du traitement

La règle en matière de publication de données permettant l'identification de la personne concernée est l'interdiction.

L'arrêté royal a cependant prévu deux exceptions, à savoir si :

> « 1° la personne concernée a donné son consentement et qu'il n'est pas porté atteinte à la vie privée de tiers ; ou
>
> 2° la publication de données à caractère personnel non codées est limitée à des données manifestement rendues publiques par la personne concernée elle-même ou ayant une relation étroite avec le caractère public de la personne concernée ou des faits dans [lesquels] celle-ci est ou a été impliquée. »

Ces exceptions sont assez logiques dès lors qu'elles sont reprises, en partie, de la loi vie privée en matière de base de légitimation des traitements (voy. *infra*).

e) Exceptions

Les principes que nous venons d'analyser en matière de traitement ultérieur à des fins historiques, statistiques ou scientifiques ne sont pas applicables « aux services et autorités visés à l'article 3, § 4, de la loi [vie privée] qui effectuent »[1] de tels traitements.

Il s'agit de services et autorités liés à « la Sûreté de l'État, par le Service général du renseignement et de la sécurité des forces armées, par les autorités visées aux articles 15, 22*ter* et 22*quinquies* de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité et l'organe de recours créé par la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité, par les officiers de sécurité et par le Comité permanent de contrôle des services de renseignements et son Service d'enquêtes, ainsi que par l'Organe de coordination pour l'analyse de la menace lorsque ces traitements sont nécessaires à l'exercice de leurs missions »[2].
Cette exception est, somme toute, logique car l'on voit difficilement de tels services et autorités soumis aux conditions de traitement ultérieur à des fins historiques, statistiques ou scientifiques et, principalement, à l'obligation d'informer la personne concernée...

1. Article 24 de l'arrêté royal.
2. Article 3, § 4, LVP.

5.3.4. Données adéquates et pertinentes au regard de la finalité

Afin de respecter le principe de finalité, il convient par ailleurs de bien sélectionner les données à caractère personnel qui vont faire l'objet d'un traitement.

Seules peuvent être traitées les données adéquates et pertinentes au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement[1]. Pour être jugées pertinentes, les données doivent présenter un lien nécessaire et suffisant avec les finalités poursuivies[2].

De nombreux formulaires, jugés à l'aune de cette exigence de pertinence des données, devraient bien être allégés en termes de données recueillies. Ainsi, pour reprendre des exemples tirés de la réalité, la date de naissance d'un client n'est pas nécessaire pour gérer sa commande ; le nom de l'employeur ne doit pas être réclamé par la police dans le document à remplir par un conducteur pris en infraction de roulage ; l'âge de l'acquisition de la propreté et la durée de l'allaitement maternel ne doivent pas figurer sur les formulaires que les services PMS font remplir à l'ensemble de la population scolaire[3].

Dans ces cas, soit les données visées sont appelées à servir en fait un autre objectif que celui annoncé, ce qui est illégal, soit le lien de pertinence avec la finalité poursuivie est trop ténu pour que les données soient jugées pertinentes, soit même inexistant. De nombreuses données sont en réalité collectées par habitude. La loi du 8 décembre 1992 est l'occasion pour de nombreuses personnes, de nombreux organismes, entreprises ou administrations de reconsidérer les habitudes de collecte de données en place et de vérifier la pertinence des données au regard des finalités poursuivies par les traitements.

5.3.5. Conservation des données limitée au regard de la finalité

La détermination de la finalité permet également de définir la durée de conservation des données dès lors que l'article 4, § 1er, 5°, de la LVP prescrit que les données à caractère personnel doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement [...] »

---

1. Les données ne peuvent pas non plus être excessives, mais cette caractéristique correspond au principe de proportionnalité et sera vue *infra*, sous le point consacré à ce principe.
2. M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreaux et Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p. 146.
3. Ces formulaires du PMS ont été « nettoyés » à la suite d'une plainte et ne contiennent plus aujourd'hui les données en question.

La durée licite de conservation des données n'est donc pas uniforme, mais dépend de la finalité du traitement des données, sous réserve des précisions apportées par l'arrêté royal du 13 février 2001 concernant la conservation de données « au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques »[1].

Dès l'instant où les données ne sont plus nécessaires pour atteindre la finalité de leur collecte ou les finalités ultérieures compatibles, le responsable du traitement est tenu soit de les effacer, soit de les anonymiser, c'est-à-dire de faire disparaître irréversiblement leur élément identifiant[2].

Le responsable du traitement doit faire cette opération de suppression ou d'anonymisation des données spontanément, et non sur demande des personnes concernées.

Cette obligation d'effacement illustre le « droit à l'oubli » qui est reconnu par là aux personnes concernées[3]. Il n'est pas légitime, pour la plupart des traitements de données, de conserver *ad vitam aeternam* les données sous une forme permettant l'identification des personnes. Dès qu'elle ne se justifie pas par un critère de nécessité, une conservation des données « pour mémoire » n'est pas légitime.

Il est à noter toutefois que les données peuvent être conservées à des fins probatoires durant une période correspondant au délai de prescription.

Il existe des traitements de données dont la finalité est telle qu'elle permet la conservation des données illimitée dans le temps. Il s'agit, par exemple, de la tenue des registres de population par les communes ou de l'archivage des documents du secteur public contenant des données à caractère personnel.

5.4. Le principe de proportionnalité

L'exigence de proportionnalité se place à deux niveaux dans la loi vie privée, à savoir la proportionnalité des données à caractère personnel, mais également la proportionnalité du traitement lui-même.

1. Article 4, § 1er, 4°, LVP.
2. Rappelons qu'il ne suffit pas de coder les données pour les anonymiser. Des données codées demeurent des données à caractère personnel tant que la clé du code est conservée (voy. *supra*).
3. C. DE TERWANGNE, « Internet privacy and the right to be forgotten/right to oblivion », *Revista de Internet, Derecho y Política*, 2012, n° 13, p. 114, also available at http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13-terwangne_eng.

5.4.1. Proportionnalité du traitement

a) L'exigence de proportionnalité

On a déjà mentionné (au point 5.3.1., c)) que la finalité du traitement de données doit être « légitime », concept qui renvoie à la nécessité de respecter le principe de proportionnalité. Si cette exigence particulière touchant à la finalité du traitement a déjà été évoquée ci-dessus, c'est parce que les exigences légales relatives à la finalité ont été présentées en un bloc sous le point réservé au principe de finalité. Il est clair toutefois que l'exigence de finalité « légitime » relève de l'application du principe de proportionnalité.

Cette exigence de finalité légitime doit se combiner avec l'exigence pour l'ensemble du traitement de respecter la règle de proportionnalité. Ainsi, la Commission européenne, intervenant dans l'affaire *Österreichischer Rundfunk* confiée à la Cour de justice, évoque « l'*examen de proportionnalité effectué en vertu de l'article 6, paragraphe 1, sous b)* [disposition équivalant textuellement à l'article 4, § 1er, 2°, de la loi belge, en d'autres mots à l'exigence de finalité légitime] »[1]. La Cour de justice des Communautés européennes, dans cette affaire, a complété cette vision en estimant qu'en présence d'un traitement de données à caractère personnel, sont légitimes les objectifs listés dans l'énumération de l'article 8, § 2, CEDH (objectifs qui peuvent justifier des atteintes à la vie privée), mais qu'il convient de vérifier le respect de l'exigence de proportionnalité contenue elle aussi à l'article 8, § 2, CEDH[2]. L'article 8, § 2, de la Convention n'admet en effet les ingérences dans le droit au respect de la vie privée que si elles constituent une mesure nécessaire dans une société démocratique à la réalisation d'une des fins énoncées. La nécessité implique non seulement que la mesure réponde à un besoin social impérieux, mais également qu'il n'existe pas de voie moins attentatoire pour réaliser l'objectif poursuivi et, enfin, que la mesure respecte « un juste rapport de proportionnalité entre les moyens utilisés et le but à atteindre »[3].

Dans un arrêt du 10 novembre 2011[4], la Cour constitutionnelle a eu l'occasion de rappeler que « toute ingérence des autorités dans le droit au respect de la vie privée [doit être] prévue par une disposition législative suffisamment précise » outre qu'elle doit répondre « à un besoin social impérieux » et qu'elle doit être « *proportionnée au but légitime qui est poursuivi* ».

La Cour européenne des droits de l'homme a également estimé que « le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échan-

---

1. C.J.C.E., arrêt du 20 mai 2003 (Österreichischer Rundfunk e.a.), C-465/00, C-138/01 et C-139/01, point 57.
2. C.J.C.E. (Österreichischer Rundfunk), préc., points 81 et s.
3. M. VAN OVERSTRAETEN et S. DEPRÉ, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, p. 688.
4. C.C., 10 novembre 2011, 166/2011, www.const-court.be, B 35.3. Il faut relever que cette exigence permet au justiciable de contrôler l'ingérence et sa légalité. Voy. également Cour eur. D.H., arrêt Rotaru c. Roumanie, 4 mai 2000, *Rev. trim. dr. h.*, 2001, pp. 137 à 183, obs. O. De Schutter.

tillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'État défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique »[1].

Dans son arrêt *Volker und Markus Scheke & Eifert*[2], la Cour de justice de l'Union européenne a considéré « que la publication sur Internet de données nominatives concernant les personnes physiques bénéficiaires d'aides agricoles constitue une ingérence dans leur droit au respect de la vie privée reconnu à l'article 7, et un traitement de données relevant de la protection garantie par l'article 8 de la Charte[3]. Si cette ingérence peut être considérée comme poursuivant un but légitime, à savoir l'accroissement de la transparence de l'utilisation des fonds communautaires de la PAC[4], elle sera finalement jugée disproportionnée par la Cour[5] »[6].

Le juge devra donc, s'il est saisi dans le cadre d'une violation de la loi vie privée, analyser le traitement afin de déterminer si la condition de nécessité/proportionnalité a effectivement été rencontrée concernant la finalité poursuivie et l'ensemble du traitement.

b) Les hypothèses de respect de la proportionnalité : les fondements légitimes des traitements de données

L'article 5 de la loi du 8 décembre 1992[7] énonce les six seules hypothèses dans lesquelles un traitement de données peut être effectué. « Ces hypothèses représentent en fait les situations dans lesquelles l'équilibre des intérêts en présence est *a priori* atteint »[8]. M.-H. Boulanger, intervenant au nom de la Commission (belge) de la pro-

1. Cour eur. D.H., arrêt S. et Marper c. Royaume-Uni, 4 décembre 2008, req. n^{os} 30562/04 et 30566/04, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90052, alinéa 125.
2. C.J.U.E. (Gr. Ch.), 9 novembre 2011 (Volker und Markus Schecke GbR et Harmut Eifert c. Land Hessen), aff. jointes C-92/09 et C-93/09. Voy. E. Degrave, « Arrêt "Volker und Markus Schecke et Eifert" : le droit fondamental à la protection des données à caractère personnel et la transparence administrative », *J.D.E.*, 2011, pp. 97 à 99, et I. Andoulsi, « L'arrêt de la Cour du 9 novembre 2012 dans les affaires jointes *Volker und Markus Schecke GbR et Hartmut Eifert c. Land d'Hessen* : une reconnaissance jurisprudentielle du droit fondamental à la protection des données personnelles ? », *C.D.E.*, vol. 47, n° 2, 2011, pp. 471 à 522.
3. Points 58 et 60.
4. Point 71.
5. Point 86.
6. C. Gayrel, « Chronique de jurisprudence en droit des technologies de l'information (2009-2011). Libertés et société de l'information. Cour de Justice de l'Union européenne, Tribunal de Première Instance et Tribunal de la Fonction publique européenne », *R.D.T.I.*, n^{os} 48 et 49, 2012, p. 107.
7. Reproduction de l'article 7 de la directive 95/46 du 24 octobre 1995.
8. C. de Terwangne, « La nouvelle loi belge de protection des données à caractère personnel », *in* P. Tabaton (dir.), *La protection de la vie privée dans la société d'information*, Cahier des Sciences morales et politiques, Paris, PUF, 2002, p. 99, disponible sur le site de l'Académie des Sciences morales et politiques, http://www.asmp.fr/travaux/gpw_internetvieprivee.htm. Dans le même sens, J. Dhont, « Le traitement des données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, 1/2000, pp. 323 et 324.

tection de la vie privée, signala, lors des discussions qui accompagnèrent le vote de la modification de la loi belge, que les situations visées par l'article 5 de la loi créent « une présomption d'équilibre d'intérêts »[1].

Les articles 4, § 1er, b), et 5 doivent être lus conjointement. Le fait de se trouver dans une des situations énoncées à l'article 5 n'implique pas que l'exigence de finalité légitime de l'article 4 soit *ipso facto* rencontrée. Les hypothèses visées dans la première disposition n'empêchent pas un contrôle sur la base de la deuxième[2]. En fait, on peut considérer que l'article 5 prévoit des situations abstraites dans lesquelles l'équilibre des intérêts en présence est normalement respecté, sans préjudice d'un contrôle concret, sur la base de l'article 4, permettant, le cas échéant, de révéler une atteinte inacceptable aux droits et intérêts de l'individu[3]. Ce n'est pas parce qu'on a le consentement d'une personne à ce que l'on traite les données la concernant (ce qui correspond à une des hypothèses de légitimité de l'article 5) que le traitement est d'office admissible. Il porte peut-être atteinte de manière disproportionnée à un intérêt collectif qui n'a forcément pas été pris en compte par la personne concernée qui n'a envisagé, comme il se doit, que ses propres droits et intérêts pour donner son consentement. La condition de finalité légitime de l'article 4, § 1er, b), n'est, dans ce cas, pas rencontrée alors même que l'article 5 est respecté. Le traitement de données envisagé doit être déclaré illégal.

Pour être admis, tout traitement de données doit donc respecter le principe de proportionnalité et reposer sur un fondement légitime, c'est-à-dire correspondre à l'une des six hypothèses énoncées par la loi. Ces hypothèses sont les suivantes.

Le consentement

La première hypothèse envisageable est celle du consentement de la personne concernée[4].

Pour être valable, le consentement doit être libre, informé et spécifique[5]. Il doit donc être :

- obtenu sans pression quelconque ;
- en connaissance de cause (la personne concernée doit notamment savoir qui effectuera quoi et pourquoi sur ses données et se rendre compte des destinataires de ses données) ; et
- ne peut être général.

---

1. *In* rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Chambre, 1998-1999, n° 1566/10, p. 47.
2. M. Van Overstraeten et S. Depre, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », *Rev. trim. dr. h.*, 2003, pp. 689 et 690.
3. M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau et Y. Poullet, *op. cit.*, p. 148, n° 41 ; J. Dhont, « Le traitement des données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, 1/2000, pp. 324 et 325.
4. Article 5, alinéa 1er, littera a, LVP.
5. Article 1er, § 8, LVP.

La forme du consentement n'est pas imposée par la loi (à la différence des traitements mettant en cause des données sensibles pour lesquels un consentement écrit est exigé, voy. *infra*). Le consentement ne doit pas nécessairement être exprès, mais, même tacite, il doit être indubitable.

Si un organisme, une entreprise ou un cabinet d'avocats décide, par exemple, de développer un site Internet présentant notamment ses membres ou dirigeants nominativement, il conviendra d'obtenir le consentement de chaque personne présentée sur le site[1].

Il est utile d'attirer l'attention sur le fait que, si le consentement de la personne concernée est un reflet du principe d'autodétermination informationnelle de l'individu tel qu'évoqué plus haut, il ne constitue cependant qu'une base de légitimation du traitement parmi d'autres et encore la plus faible de ces bases, dès lors que la personne concernée peut retirer son consentement sans devoir motiver sa décision. C'est aussi une base fragile dont la qualité n'est pas toujours garantie, car le sujet est susceptible de faire l'objet de pressions – même inconscientes ou culturelles – diverses au moment de donner son consentement.

D'autres hypothèses sont admises, dans lesquelles on peut se passer du consentement des personnes concernées.

Le contrat

Le traitement de données à caractère personnel peut être effectué lorsque le traitement s'avère « nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci »[2].

Le cadre contractuel peut donc légitimement servir de fondement aux traitements de données à caractère personnel. Les contrats de travail, ceux passés avec une banque, une assurance, une société de vente à distance ou un voyagiste, par exemple, sont autant de cadres justifiant de nombreux traitements de données à caractère personnel.

> « Entrent clairement dans cette hypothèse les traitements effectués dans le cadre de la relation liant l'avocat à son client. Cela couvre même les hypothèses de remplacement de l'avocat aux audiences, dès lors que ces remplacements permettent une bonne exécution du contrat. Notons cependant que cette hypothèse n'autorise pas à traiter des données relatives à des individus qui ne sont pas eux-

1. Voy. C. DE TERWANGNE, « Affaire Lindqvist ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », note sous C.J.C.E., arrêt du 6 novembre 2003, *R.D.T.I.*, 2004, n° 19, p. 95.
2. Article 5, alinéa 1er, littera b, de la loi du 8 décembre 1992.

mêmes clients de l'avocat. On ne peut dès lors s'appuyer sur ce fondement pour recueillir des informations sur la partie adverse »[1].

Il faut toutefois répondre à deux conditions pour que ce fondement soit valablement invoqué.

Il faut tout d'abord que la personne concernée soit partie au contrat en question ou qu'elle ait demandé que soient prises des mesures précontractuelles nécessitant un traitement de données. Le contrat ne peut donc impliquer des données à caractère personnel concernant une personne qui n'y est pas partie. Si cela arrive, un autre fondement doit couvrir le traitement de telles données.

La deuxième condition consiste en ce que le traitement de données soit véritablement **nécessaire** à l'exécution du contrat en question ou des mesures précontractuelles. Ainsi, la mise en place de caméras de surveillance dans les différentes zones d'une banque ne peut être jugée nécessaire à l'exécution des contrats liant la banque à ses clients. De même, la promotion par une agence de voyages des city-trips qu'elle organise auprès de ses clients ayant réservé par ses soins un week-end à Barcelone ne peut être considérée comme nécessaire à l'exécution du contrat de voyage relatif à Barcelone. Ces opérations ne sont pas illégales pour autant, mais, pour être admissibles, elles doivent s'appuyer sur un autre fondement légitime que l'exécution du contrat (la balance d'intérêts – voy. *infra* – dans le cas de la banque et le consentement dans le cas de l'agence de voyages).

L'intérêt vital de la personne concernée

Un traitement de données à caractère personnel « nécessaire à la sauvegarde de l'intérêt vital de la personne concernée »[2] est également légitime aux yeux de la loi.

Cela couvre l'hypothèse évidente où une personne accidentée nécessite des soins induisant de traiter ses données relatives, par exemple, à son groupe sanguin. Or, si elle a perdu connaissance, elle ne peut manifester son consentement. Ce sera donc en se fondant sur cette hypothèse-ci que le traitement pourra avoir lieu.

L'obligation légale

Le traitement de données à caractère personnel peut encore avoir lieu s'il est « nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance »[3].

---

1. C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *in Cabinet d'avocats et technologies de l'information : balises et enjeux*, coll. Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005 pp. 159 et 160.
2. Article 5, alinéa 1er, littera d, de la loi du 8 décembre 1992.
3. Article 5, alinéa 1er, littera c, de la loi du 8 décembre 1992.

L'ensemble des traitements du secteur public entre dans cette hypothèse de légitimité. Le principe de légalité qui gouverne l'administration impose effectivement que les missions confiées à l'administration aient une base légale[1]. En effet, « tout acte du Roi doit se fonder sur des règles émanant d'une autorité supérieure, le constituant ou, à défaut, le législateur »[2].

Pour être retenue comme justifiant des traitements de données, une norme doit répondre aux exigences que la Cour européenne des droits de l'homme a fait découler de l'article 8, § 2, CEDH : elle doit être accessible et prévisible. Rappelons que, pour être prévisible, une norme doit être suffisamment détaillée pour qu'à sa lecture, on soit à même d'envisager les atteintes basées sur le paragraphe 2, ce qui signifie dans le cas présent qu'on se rende compte des traitements de données qui auront lieu.

Les collectes et enregistrements de certaines données sur les employés par l'employeur et leur communication à l'administration en charge de la sécurité sociale sont imposés par la législation. Ces opérations sont donc parfaitement légitimes. Il en est de même, pour prendre un exemple dans un autre registre, de l'obligation pour les médecins ayant mis des implants dans le corps de leurs patients d'indiquer pour chaque patient en question, dans le registre des implants récemment créé, le type d'implants, afin d'assurer une traçabilité de ces derniers.

Il est impératif, ici comme dans le cas d'un contrat, que les opérations effectuées sur les données (enregistrement, utilisation, transfert...) soient véritablement nécessaires pour répondre à l'obligation légale.

La mission d'intérêt public

D'une manière très proche, les traitements « nécessaire[s] à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées »[3] correspondent aussi à une hypothèse de traitements légitimes aux yeux de la loi.

L'enregistrement et la gestion des abonnés par les sociétés publiques de transports en commun (SNCB pour les trains ou TEC pour les bus par exemple) se justifient pleinement sur cette base. Par contre, la mise en œuvre des cartes MoBIB dans le réseau de métro bruxellois n'a pas été sans susciter des problèmes de traitement illégitime de données à caractère personnel. En effet, en quoi une carte de tickets de

1. Voy. article 105 Const.
2. E. DEGRAVE et Y. POULLET, « L'externalisation de l'administration, les nouvelles technologies et la protection de la vie privée », *J.T.*, 2008, p. 280. Pour d'amples développements sur le principe de légalité et son implication en termes de protection des données à caractère personnel, voy. E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, thèse de doctorat, 2013, à paraître.
3. Article 5, alinéa 1er, littera e, de la loi du 8 décembre 1992.

voyage (et non pas un abonnement) nécessite-t-elle de comporter un identifiant personnel[1] ?

Ici aussi, tout comme dans les cas précédents, il faut vérifier si les opérations effectuées sur les données (enregistrement, utilisation, transfert...) sont véritablement nécessaires pour répondre à l'obligation légale.

La balance d'intérêts

Enfin, la loi propose une dernière hypothèse dans laquelle le traitement de données à caractère personnel est légitime, c'est le cas du traitement « nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée »[2].

Cette hypothèse est en fait une hypothèse « fourre-tout » destinée à permettre une série de traitements de données qui sont admissibles, car légitimes, mais ne peuvent être envisagés théoriquement de manière exhaustive sous peine de ne pas couvrir tous les cas qui mériteraient de figurer dans la liste. Cette dernière hypothèse correspond donc à l'exercice de mise en balance des intérêts et droits en présence sans que le législateur ait cette fois, comme dans les autres hypothèses, donné corps au résultat équilibré issu d'une telle mise en balance.

Il reviendra donc dans un premier temps au responsable du traitement d'effectuer lui-même la mise en balance et, s'il estime que la mise en œuvre du traitement de données qu'il envisage sert un intérêt supérieur à celui de la personne concernée ainsi qu'aux droits et libertés de celle-ci, il conclura que son traitement est légitime.

La personne concernée pourra, quant à elle, contester le résultat de cette mise en balance et estimer que ses intérêts, droits et libertés prévalent sur l'intérêt poursuivi par le responsable. La loi lui octroie pour ce faire un droit d'opposition (voy., *infra*, point 6.4.).

En dernier ressort, si les deux intervenants ne se mettent pas d'accord à la suite d'une opposition manifestée par la personne concernée, ils pourront s'adresser à la Commission de la protection de la vie privée pour avoir son avis sur les intérêts prévalant dans la situation en litige. Cet avis n'ayant pas de force obligatoire, c'est au tribunal qu'il reviendra de prononcer le dernier mot sur le résultat d'une mise en balance des intérêts en jeu.

---

1. Sur cette question, voy. F. Dumortier, A. Rouvroy, F. Standaert et F. Koeune, « Carte MoBIB : un bon exemple de mauvaise mise en œuvre », *Bruxelles en mouvements*, n° 240, 10 septembre 2010, pp. 9 et s., également disponible à l'adresse http://www.crid.be/pdf/crid5978-/6557.pdf.
2. Article 5, alinéa 1er, littera e, de la loi du 8 décembre 1992.

5.4.2. Proportionnalité des données

L'article 4, 3°, prescrit qu'outre d'être adéquates et pertinentes ainsi que cela a été mentionné antérieurement, les données à caractère personnel doivent être « non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ».

Cela signifie que « [d]es données pertinentes au regard de l'objectif poursuivi mais induisant une atteinte excessive à la personne concernée par rapport à l'intérêt qu'elles présentent pour la personne qui souhaite les traiter, ne peuvent être recueillies »[1]. En outre, le responsable de traitement ne pourra pas collecter des données qui ne seraient pas nécessaires pour atteindre la finalité qu'il a préalablement déterminée, dans la mesure où moins de données ou des données moins attentatoires à la personne concernée permettent d'atteindre cette finalité.

Un arrêt a été rendu par la Cour constitutionnelle dans le cadre d'une requête en annulation déposée contre la loi du 21 janvier 2010 modifiant la loi du 25 juin 1992 sur le contrat d'assurance terrestre en ce qui concerne les assurances du solde restant dû pour les personnes présentant un risque de santé accru. En vertu de cette loi, la Commission des assurances devait établir un code de bonne conduite à défaut de quoi le Roi était habilité à régler la question des questionnaires médicaux dans le cadre des assurances du solde restant dû pour les personnes présentant un risque de santé accru. La Cour a considéré que « le législateur a pu estimer que l'utilisation de ces questionnaires devait être réglementée afin d'éviter que, dans le cadre de la conclusion d'un contrat d'assurance, des questions soient posées qui ne sont pas pertinentes ou qui sont excessives et qu'il soit ainsi porté atteinte de manière disproportionnée au droit au respect de la vie privée des intéressés. Il a également pu estimer que le fait que les assureurs exigent un examen médical complémentaire et demandent les résultats de celui-ci, en plus de l'utilisation d'un questionnaire médical, pouvait constituer une restriction disproportionnée du droit au respect de la vie privée de l'intéressé dans les cas où le montant assuré demeure limité »[2].

Elle a ainsi clairement rappelé que la proportionnalité devait être analysée au niveau des données afin d'éviter que des données non nécessaires à la finalité soient traitées[3].

La Cour européenne des droits de l'homme a également précisé que « [l]e droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont

1. C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *in Cabinet d'avocats et technologies de l'information : balises et enjeux*, coll. Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005 p. 162.
2. C.C. (166/2011), 10 novembre 2011, www.const-court.be, B.16.7.
3. S. Hallemans, M. Van Winckel et J.-M. Van Gyseghem, « Libertés et société de l'information », *RDTI*, 48-49, p.76

conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (préambule et article 5 de la Convention sur la protection des données et principe 7 de la recommandation R(87)15 du Comité des Ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police) »[1].

La Commission de la protection de la vie privée a eu l'occasion d'insister sur la nécessité de restreindre le nombre de données faisant l'objet d'un traitement (une transmission hors des services médicaux, dans le cas soumis à la Commission) dans son avis sur le « Résumé minimal psychiatrique »[2]. En l'occurrence, le transfert au ministre d'une grande quantité de données relatives à la santé risquerait de miner la confiance des patients dans leurs médecins.

Nous constatons donc, et pour rappel, que la détermination de la finalité est primordiale pour permettre, d'une part, au responsable du traitement de déterminer les données à caractère personnel qu'il collectera et traitera, ainsi que la durée de conservation de celles-ci, et, d'autre part, à la personne concernée d'exercer son contrôle via les droits qui lui sont offerts par la loi vie privée.

5.5. La protection accrue des données sensibles

5.5.1. Les données sensibles

a) La définition de la loi vie privée

Trois sous-catégories

On a déjà signalé antérieurement que l'identification d'une catégorie particulière de données à caractère personnel auxquelles on réserve une protection plus élevée est liée aux risques accrus de porter préjudice aux individus sur la base du traitement de ces données. C'est principalement le risque de discriminations illégitimes ou arbitraires qui est lié à ces données qui justifie le traitement différencié qui leur est accordé[3]. De telles données présentent, en outre, un risque d'affecter la sphère la plus intime

1. Cour eur. D.H., arrêt S. et Marper c. Royaume-Uni, 4 décembre 2008, req. n^{os} 30562/04 et 30566/04, § 103.
2. C.P.V.P., avis n° 12/2002 du 21 mars 2002 relatif au projet d'arrêté royal fixant les règles suivant lesquelles certaines données statistiques minimales psychiatriques doivent être communiquées au ministre qui a la Santé publique dans ses attributions.
3. Voy. J. RINGELHEIM, « Recueil des données personnelles et lutte contre les discriminations. Une tension nécessaire entre non-discrimination et vie privée », *in Les nouvelles lois luttant contre la discrimination*, Bruges, La Charte, 2008, pp. 91 et s.

des sujets de données ainsi qu'un risque sérieux de dommage, en cas d'abus, pour la personne concernée[1].

La catégorie des données qualifiées de « sensibles » est visée par les articles 6, 7 et 8 de la LVP, qui réservent un régime plus protecteur à ces données. Ainsi qu'on l'a déjà exposé plus haut, ces données rassemblent en fait trois sous-catégories de données :

- les données à caractère personnel « qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, et les données relatives à la vie sexuelle », données qualifiées de sensibles au sens strict (visées par l'art. 6 de la loi) ;
- les données relatives à la santé (visées à l'art. 7 LVP) ; et
- les données à caractère personnel « relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté », communément reprises sous l'appellation de « données judiciaires » (visées à l'art. 8 de la loi)[2].

Difficulté d'application de la définition

On rappelle aussi ici ce qui a été dit antérieurement sur la difficulté engendrée par la formulation très large des première et deuxième sous-catégories des données sensibles. À ce stade, il est utile de répéter l'ambiguïté des articles 6 et 7 par rapport à leur qualification même. En effet, ces deux articles sont applicables dès l'instant où un traitement porte sur les données visées, même si le traitement ne vise pas les données à caractère personnel pour l'élément sensible qu'elles comportent.

Par exemple, le site Internet d'une société comprend un annuaire des personnes travaillant en son sein, annuaire accompagné de leurs photos. Si un des employés apparaît sur la photo en portant des signes religieux, le traitement de cette photo, étant une donnée à caractère personnel, devrait tomber dans le champ d'application de l'article 6, dès lors que la donnée est relative à l'appartenance religieuse de la personne concernée, alors qu'il importe peu au responsable du traitement que cette

1. Voy. les développements consacrés à la raison d'être de la catégorie spécifique des données sensibles dans la contribution du présent ouvrage sur la Convention 108 du Conseil de l'Europe relative à la protection des personnes à l'égard des traitements automatisés de données à caractère personnel (C. DE TERWANGNE et J.-PH. MOINY, « La Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et les concepts fondamentaux de la protection des données », point 6).
2. La catégorie des « données judiciaires » telle qu'énoncée dans la loi belge est plus large que la catégorie de données visée à l'article 8, § 5, de la directive 95/46 qui dispose que « [l]e traitement *de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté* ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. Les États membres peuvent prévoir que les *données relatives aux sanctions administratives ou aux jugements civils* sont également traitées sous le contrôle de l'autorité publique » (nous soulignons).

personne soit d'une religion ou d'une autre. Cela implique cependant que le traitement devrait répondre à une des causes de légitimation prévues à l'article 6.

Dans la même ligne que cet exemple, le Groupe de l'article 29 s'est penché sur la question des informations sensibles pouvant découler d'une photographie d'une personne identifiable. Sa conclusion est la suivante : « Dans certains États membres de l'Union européenne, les images de personnes concernées sont considérées comme une catégorie spéciale de données personnelles puisqu'elles peuvent être utilisées pour distinguer l'origine raciale/ethnique ou pour en déduire des croyances religieuses ou des données relatives à la santé. Le groupe de travail ne considère pas, en général, les images sur Internet comme des données sensibles, sauf si elles sont clairement utilisées pour révéler des données sensibles sur des personnes »[1].

Il eût été plus opportun de rédiger ces articles afin de viser le contenu des données, de manière à ce que l'interdiction de traitement soit le principe pour les données à caractère personnel sensibles et celles relatives à la santé si elles sont traitées *pour ce qu'elles révèlent ou contiennent*. Cela enlèverait l'ambigüité relevée ci-dessus et que nous retrouvons également dans la directive 95/46[2]. Il revient donc au juge d'être attentif au contexte du traitement avant de conclure à un traitement soumis aux articles 6 ou 7 de la loi[3].

Les données relatives à la santé

La loi ne définit plus, contrairement à la version de 1992, ce qu'il faut entendre par « données relatives à la santé », si ce n'est que l'Exposé des motifs précise que cette notion est plus large que celle de « données médicales » précédemment utilisée[4]. Elle est en fait également plus restreinte sur certains aspects car elle ne couvre plus les données qui *révèlent* un état de santé, mais seulement celles *relatives* à la santé, qui s'y rapportent[5].

Jurisprudence et doctrine[6] ont cependant éclairci quelque peu la notion. Ainsi, J. Dhont apporte le commentaire suivant sur cette notion : « On est d'avis que les "données relatives à la santé" couvrent une réalité plus ample que la notion de donnée médicale dans la loi précédente. Aussi la recommandation R (97)5 du Comité des Ministres du Conseil d'Europe, qui utilise encore l'expression "données médicales"

1. Groupe de l'article 29, avis 5/2009 du 12 juin 2009 sur les réseaux sociaux en ligne (*WP* 163).
2. Article 8 de la directive 95/46.
3. Voy., dans le même sens, Th. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 386, spéc. la note 106.
4. Exposé des motifs, *Doc. parl.*, Chambre, 1997-1998, n° 1566/1, p. 38.
5. Voy. M. Boulanger, S. Callens et S. Brillon, « La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001 », *T. Gez.-Rev. dr. santé*, 2000-2001, p. 331.
6. Notamment M. Boulanger, S. Callens et S. Brillon, *op. cit.*, pp. 326 et s. ; M. Parisse et V. Verbruggen, « Secret professionnel et vie privée : les traitements de données à caractère personnel (relatives à la santé) couvertes par le secret professionnel », *R.D.T.I.*, 2006, pp. 15 et s.

contient une définition large : toutes les données à caractère personnel relatives à la santé d'une personne. Elle [la définition] se réfère également aux données ayant un lien manifeste et étroit avec la santé ainsi qu'aux données génétiques »[1]. Pour cet auteur, il suffit que l'information soit en lien ou concerne la santé d'une personne pour que l'on puisse parler de données relatives à la santé. « En conséquence, non seulement les informations médicales "dures" tomberont sous la définition, mais également celles qui reçoivent une connotation médicale par le contexte »[2].

Il est à noter que la personne concernée par des données relatives à la santé est le patient lui-même, et non ses héritiers. Cela a été affirmé par le Tribunal de première instance de Bruxelles qui, dans le cadre de l'article 7 de la LVP, a estimé que les ayants droit d'un patient décédé doivent être considérés comme des tiers par rapport à la personne concernée qu'était le défunt[3].

Données judiciaires

La définition belge des données judiciaires est plus large que celle inscrite dans la directive 95/46 qui ne visait pas les données se rapportant à des suspicions et des poursuites, pas plus que celles relatives à des litiges soumis aux cours et tribunaux[4]. Selon l'Exposé des motifs du projet de loi qui allait aboutir à la modification de la loi du 8 décembre 1992, l'introduction des suspicions et des poursuites dans cette catégorie de données sensibles « montre que l'article 8 ne s'applique pas uniquement aux condamnations pénales mais également aux données dont il ressort qu'une personne est soupçonnée ou poursuivie pour un délit »[5].

b) Applications

Données sensibles au sens strict

À l'occasion d'une affaire initiée par une personne ayant reçu de nombreux courriels du Front National du fait qu'elle figurait sur une *mailing list* établie par ce parti, la Cour d'appel de Bruxelles analysa que « le fichier dans lequel figurait la partie civile n'était pas de nature à révéler, en particulier, les opinions politiques de la partie civile, dès lors qu'il n'était pas destiné à répertorier les membres ou les sympathisants du parti Front National mais bien les personnes physiques ou morales souhaitant être informées des activités du parti, par intérêt professionnel, par sympathie ou même par

1. J. Dhont, « Le traitement des données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, 1/2000, p. 302.
2. J. Dhont, *op. cit.*, p. 302, note 33. Voy. également J. Dhont et Y. Poullet, *De verwerking van medische persoonsgegevens voor wetenschappelijke en statistische doeleinden*, D.W.T.C., 1998, pp. 28 et s.
3. Civ. Bruxelles, 25 mars 2005, *J.L.M.B.*, 2005, p. 1197.
4. Th. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, p. 388.
5. Exposé des motifs, *Doc. part.*, Chambre, 1997-1998, n° 1566/1, p. 42.

simple curiosité »[1]. Les adresses répertoriées dans la liste ne constituaient donc pas des données relatives à des opinions politiques étant donné que le fichier en question n'était pas exclusivement constitué d'adresses de membres ou de partisans du Front National. D'après la Cour, ce fichier comprenait d'ailleurs des adresses de courrier électronique appartenant à des personnes qui n'adhéraient indubitablement pas aux opinions promues par ce parti.

Données relatives à la santé

Dans l'affaire *Lindqvist* confiée à la Cour de justice de l'Union européenne[2], le ministère public, suivi par le juge suédois qui prononça la condamnation initiale à l'origine de l'affaire, a reproché à M^me^ Lindqvist d'avoir traité sans autorisation des données à caractère personnel sensibles, « à savoir celles relatives à une blessure au pied et à un congé de maladie [d'une de ses collègues] »[3]. La juridiction d'appel voulut obtenir la confirmation que l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue bien une donnée à caractère personnel relative à la santé au sens de l'article 8 de la directive. La Cour de Luxembourg ne tergiversa pas sur cette question de détermination de cette catégorie particulière de données. Elle répondit qu'il convient de réserver une interprétation large à l'expression « données relatives à la santé ». Cela conduit à faire entrer dans cette catégorie les informations portant sur « tous les aspects, tant physiques que psychiques, de la santé d'une personne »[4]. Et la Cour de conclure que la mention du pied blessé et du congé de maladie subséquent relève effectivement de cette catégorie.

Selon le Conseil d'État, « un test d'haleine implique le traitement de données de santé »[5].

Données judiciaires

Il a été jugé, dans le cadre de la base de données Datassur, que « [l]a mention "risque résilié après plusieurs sinistres" » ne constituait pas, en tant que telle, une donnée judiciaire au sens de l'article 8 de la loi du 8 décembre 1992[6].

La Commission de la protection de la vie privée a spécifié qu'un extrait du casier judiciaire et son contenu constituent des données judiciaires au sens de l'article 8 de la LVP[7].

---

1. Bruxelles (11^e^ ch. corr.), 17 mars 2010, *R.D.T.I.*, n° 42/2011, p. 53.
2. C. DE TERWANGNE, « Arrêt *Lindqvist* ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », note sous C.J.C.E., 6 novembre 2003, *R.D.T.I.*, 2004, n° 19, pp. 67 à 99.
3. Point 15 de l'arrêt.
4. Point 50 de l'arrêt.
5. C.E., 27 octobre 2005, n° 150.861, cité par J.-PH. MOINY et J.-M. VAN GYSEGHEM, « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T.I.*, 2009, p. 90.
6. Civ. Bruxelles (8^e^ ch.) 11 juin 2004, *Bull. ass.*, 2005, pp. 47 à 51, spéc. p. 51, citant Prés. Bruxelles, 19 décembre 2000, *in Bull. ass.*, 2001, sommaire, p. 266.
7. C.P.V.P., avis n° 10/2011 du 25 mai 2011 relatif au projet de décret organisant l'accueil préscolaire d'enfants.

5.5.2. Le régime d'interdiction de traitement sauf exceptions

a) Le principe : l'interdiction de traitement

Les articles 6, 7 et 8 de la LVP mettent en place un régime d'interdiction de traitement compte tenu du fait que les données visées sont susceptibles *in se* de porter atteinte aux libertés fondamentales ou à la vie privée.

b) Les exceptions

La loi prévoit des cas dans lesquels le traitement des trois catégories de données sensibles est admis, mais elle invite le Roi à fixer les conditions particulières auxquelles doit alors satisfaire le traitement des données.

On attire l'attention sur le fait que, si l'on peut traiter les données des deux premières catégories de données sensibles avec le consentement des personnes concernées, cela n'est pas admis pour le traitement de données « judiciaires ». Les possibilités de traitement de ces dernières données sont d'ailleurs beaucoup plus restreintes que pour les données sensibles au sens strict et pour les données relatives à la santé.

On relève également que la notion de nécessité est omniprésente dans les hypothèses d'exceptions admises.

Pour les traitements de données visées aux articles 6 et 7[1]

Les données sensibles *stricto sensu* et les données relatives à la santé peuvent être traitées avec le consentement écrit – alors que l'écrit n'est pas requis dans le cadre de l'article 5 de la loi – de la personne concernée[2]. Rappelons que, pour être valable, le consentement doit avoir été donné sans aucune pression (consentement libre), en toute connaissance de cause (consentement éclairé) et de manière spécifique et non générale (consentement spécifique)[3]. La loi précise que, pour les traitements de données visés aux articles 6 et 7, le consentement donné par une personne concernée doit pouvoir à tout moment être retiré par celle-ci.

Cette exception n'est toutefois plus valable lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne concernée ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement l'empêchant de refuser librement son consentement. Dans une telle situa-

---

1. Pour des développements sur les exceptions dont bénéficient les traitements de données relatives à la santé, particulièrement le traitement avec le consentement du patient, voy. M. PARISSE et V. VERBRUGGEN, « Secret professionnel et vie privée : les traitements de données à caractère personnel (relatives à la santé) couvertes par le secret professionnel », *R.D.T.I.*, 2006, pp. 39 et s.
2. Articles 6, § 2, a), et 7, § 2, a), de la loi du 8 décembre 1992.
3. Article 1er, § 8, de la loi du 8 décembre 1992.

tion, le consentement écrit est tout de même admis comme justifiant le traitement si celui-ci vise à octroyer un avantage à la personne concernée[1].

Les données sensibles de l'article 6 et les données relatives à la santé peuvent, en outre, être traitées[2] :

- si c'est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'un tiers alors que la personne concernée est dans l'impossibilité de donner son consentement ;
- s'il est nécessaire à des fins médicales[3] ;
- si le traitement porte sur des données manifestement rendues publiques par la personne concernée ;
- si le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- s'il est nécessaire à des recherches scientifiques ;
- si cela est nécessaire au vu des obligations et des droits du responsable du traitement en matière de droit du travail ;
- s'il est nécessaire en vue de l'application de la sécurité sociale ;
- s'il est rendu obligatoire par une norme législative pour un motif important d'intérêt public.

Les seules données sensibles visées à l'article 6 peuvent, en outre, être traitées dans le cadre des activités de tout organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale pourvu que le traitement se rapporte aux seuls membres ou aux personnes entretenant des contacts réguliers avec cet organisme et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

Les données sensibles au sens strict peuvent aussi faire l'objet d'un traitement dans le cas où ce traitement serait effectué par des associations dotées de la personnalité juridique ou par des établissements d'utilité publique qui ont pour objet social principal la défense et la promotion des droits de l'homme et des libertés fondamentales, en vue de la réalisation de cet objet, à condition que ce traitement soit autorisé par le Roi, par arrêté délibéré en Conseil des ministres, après avis de la Commission de la

1. Article 27 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Voy., sur ce point, C. de Terwangne et S. Louveaux, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.*, 2001, pp. 459 et 460.
2. Articles 6, § 2, a), et 7, § 2, a), de la loi du 8 décembre 1992.
3. Plus précisément si le traitement « est nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et le traitement est effectué sous la surveillance d'un professionnel des soins de santé » (art. 6, § 2, j), et 7, § 2, j), de la loi du 8 décembre 1992). Le professionnel des soins de santé et ses préposés ou mandataires sont soumis au secret.

protection de la vie privée. Le législateur a pensé ici aux cas légitimes de traitement de données sensibles par une association comme Amnesty International[1].

On citera encore l'autorisation particulière qui est accordée pour les traitements de données relatives à la vie sexuelle. Ainsi, aux termes de l'article 6, § 3, « sans préjudice de l'application des articles 7 et 8 de la loi, le traitement de données à caractère personnel concernant la vie sexuelle est autorisé lorsque le traitement est effectué par une association dotée de la personnalité juridique ou par un établissement d'utilité publique, qui a pour but statutaire principal l'évaluation, la guidance et le traitement des personnes dont le comportement sexuel peut être qualifié d'infraction et qui est agréé et subventionné par l'autorité compétente en vue de la réalisation de ce but ; ces traitements, qui doivent être destinés à l'évaluation, la guidance et le traitement des personnes visées dans le présent paragraphe et qui ne peuvent porter que sur des données à caractère personnel qui, pour autant qu'elles sont relatives à la vie sexuelle, concernent les personnes visées dans le présent paragraphe, sont soumis à une autorisation spéciale individuelle accordée par le Roi, dans un arrêté royal délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée. » Cette disposition vise notamment à permettre les activités de traitement de données relatives à la vie sexuelle par les services spécialisés dans la guidance et le traitement des délinquants sexuels. Ces services sont appelés à donner un avis avant la libération de tout interné pour des faits d'abus sexuel, accomplis sur un mineur ou impliquant sa participation[2].

Les données relatives à la santé visées à l'article 7, quant à elles, peuvent être également traitées lorsque cela est nécessaire à la promotion et à la protection de la santé publique (dépistage...) et lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée.

Deux garanties particulières sont prévues par le législateur **pour les traitements de données relatives à la santé** qu'il autorise.

Premièrement, le traitement des données à caractère personnel relatives à la santé doit impérativement être effectué **sous la responsabilité d'un professionnel des soins de santé** qui sera, ainsi que ses préposés ou mandataires, tenu au secret. Il n'y a que dans le cas d'un consentement écrit de la personne concernée ou lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée que cette exigence ne doit pas être rencontrée.

La notion de « professionnel des soins de santé » a été accueillie comme une amélioration par rapport à la notion de « praticien de l'art de guérir » qui était reprise dans la

1. Exposé des motifs, *Doc. parl.*, Chambre, 1997-1998, n° 1566/1, p. 36.
2. Voy. article 20*bis* de la loi du 9 avril 1930 de défense sociale à l'égard des anormaux et des délinquants d'habitude, inséré par l'article 8 de la loi du 13 avril 1995 relative aux abus sexuels à l'égard des mineurs.

première version de la loi du 8 décembre 1992. Cette première notion était en effet très restrictive[1] et ne permettait pas de couvrir toutes les hypothèses légitimes nécessitant le traitement de données relatives à la santé[2]. En même temps, si la notion de « praticien de l'art de guérir » n'était pas opportune, celle de « professionnel des soins de santé » présentait, elle aussi, des défauts dont celui, majeur, de n'être pas connue ni définie au moment de l'adoption de la loi[3]. Aujourd'hui, on peut renvoyer à l'arrêté royal n° 78 relatif à l'exercice des professions des soins de santé[4].

Deuxièmement, **les données à caractère personnel relatives à la santé doivent par principe être collectées auprès de la personne concernée**. Elles ne peuvent être collectées auprès d'autres sources qu'à la condition que cela soit nécessaire aux fins du traitement ou que la personne concernée ne soit pas en mesure de fournir les données elle-même[5].

Applications

Le Conseil d'État a estimé qu'en vertu de l'article 7, § 2, de la loi du 8 décembre 1992, « un agent ne peut être soumis à un [test d'haleine] que moyennant son consentement écrit ». En outre, en application de l'article 7, § 4, alinéa 1er, « de tels tests ne peuvent être réalisés que par un professionnel des soins de santé qui est tenu au secret y compris vis-à-vis de l'autorité qui est seulement autorisée à savoir si l'agent est apte ou non à exercer ses fonctions. » Cela n'était pas le cas en l'espèce et conduisit le Conseil d'État à conclure à l'illicéité du traitement.[6]

En matière d'assurance, il a été jugé que l'envoi par une compagnie d'assurances de formulaires d'assurance fusionnés avec un questionnaire médical, sans mesures techniques de protection, impliquait qu'une partie du traitement des données médicales échappait à la responsabilité exclusive d'un professionnel des soins de santé. Le traitement fut donc considéré comme illicite par le président du tribunal[7].

---

1. Elle est définie légalement et ne couvre que les médecins, dentistes, pharmaciens et sages-femmes.
2. « On pense en particulier aux personnes comme les infirmières opérant à domicile (ou les kinésithérapeutes), amenées à prodiguer des soins à des patients et logiquement à traiter des données relatives à la santé sans toutefois disposer de la qualité de praticien de l'art de guérir » (M. Boulanger, S. Callens et S. Brillon, « La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001 », *T. Gez.-Rev. dr. santé*, 2000-2001, p. 331).
3. M. Boulanger, S. Callens et S. Brillon, *op. cit.*, p. 331 ; J. Herveg, M.-N. Verhaegen et Y. Poullet, « Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé », *Rev. dr. santé*, 2002-2003, p. 64 ; Th. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution », *op. cit.*, note 135.
4. Arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé (intitulé modifié par l'article 27 de la loi du 10 août 2001 portant des mesures en matière de soins de santé). Voy. aussi Exposé des motifs, *Doc. parl.*, Chambre, 1997-1998, n° 1566/1, p. 39.
5. Voy., sur ce dernier point, la réflexion de Thierry Léonard et Yves Poullet (Th. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, p. 388).
6. C.E., 27 octobre 2005, n° 150.861.
7. Prés. Comm. Bruxelles, 16 juin 2003, *D.C.C.R.*, 2004, p. 107. Dans le cas d'espèce, l'exemplaire destiné au courtier apportant le contrat à Fortis AG comprenait le questionnaire médical. Ce qui favorisait la non-confidentialité des données sensibles. En outre, les documents émanaient de Fortis AG et non des intermédiaires avec lesquels celle-ci travaillait. Une partie du traitement des données médicales échappait ainsi à la responsabilité exclusive d'un professionnel des soins de santé.

Le Groupe de l'article 29 a précisé, concernant les services de réseaux sociaux, qu'« [e]n tant que responsables du traitement des données, les services de réseaux sociaux (SRS) ne peuvent pas traiter des données sensibles concernant les membres ou les non-membres du réseau sans leur consentement explicite. Si un SRS fait figurer sur les formulaires d'inscription des questions portant sur des données sensibles, le SRS doit indiquer très clairement qu'il est facultatif d'y répondre »[1].

Par ailleurs, ce groupe de travail s'est également penché sur les pratiques mises en place en matière de publicité comportementale en ligne[2]. Le groupe consultatif considère qu'il existe un grave risque de porter atteinte aux données à caractère personnel si ce type d'informations est utilisé à des fins de diffusion de publicités comportementales. Tout ciblage des personnes concernées sur la base d'informations sensibles ouvrirait la voie à des abus. En outre, étant donné la nature sensible de ces informations et les situations potentiellement gênantes qui pourraient survenir si des personnes recevaient des publicités qui révèlent, par exemple, leurs préférences sexuelles ou leur activité politique, l'offre ou l'utilisation de catégories de centres d'intérêt révélant des données sensibles doit être découragée.

Pour les traitements de données visées à l'article 8

Le nombre d'exceptions prévues pour traiter ces données est très faible par rapport à celles prévues aux articles 6 et 7. En effet, l'on passe de plus d'une dizaine d'exceptions à seulement cinq cas admis. Cela démontre l'extrême sensibilité de ces données à caractère personnel qui doivent être protégées de manière encore plus forte.

Les données « judiciaires » peuvent être traitées :

- si cela est nécessaire à l'exercice des tâches d'une autorité publique ou d'un officier ministériel ;
- si c'est nécessaire à la réalisation de finalités fixées par ou en vertu de la loi ;
- pour la gestion de contentieux ;
- pour la défense de clients par les avocats ou d'autres conseils juridiques ;
- pour les nécessités de la recherche scientifique.

1. Groupe de l'article 29, avis 5/2009 du 12 juin 2009 sur les réseaux sociaux en ligne (*WP* 163).
2. Groupe de l'article 29, avis 2/2010 sur la publicité comportementale en ligne (*WP* 171).

c) Les garanties supplémentaires à observer

Pour toutes les hypothèses présentées ci-dessus, des garanties supplémentaires, fixées par le Roi aux articles 25 et 26 de l'arrêté royal du 13 février 2001, sont à observer[1] :

- selon l'article 25 de l'arrêté royal, le responsable du traitement doit désigner les catégories de personnes ayant accès aux données et décrire de manière précise leur fonction par rapport au traitement des données. Cela n'oblige pas le responsable du traitement à désigner les personnes par leur nom, mais plutôt à établir des profils d'accès. Cette liste doit être tenue à la disposition de la Commission de la protection de la vie privée ;
- les personnes autorisées à accéder aux données sensibles, médicales ou judiciaires doivent être tenues au respect du caractère confidentiel des données par une obligation statutaire ou légale, ou par une obligation contractuelle équivalente (art. 25, 3°, de l'arrêté royal)[2] ;
- Lors de l'information de la personne concernée imposée en vertu de l'article 9 de la loi ou dans sa déclaration à la Commission de la protection de la vie privée (voy. *infra*), le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement des données. Lorsqu'il était au stade du projet, le texte de l'arrêté royal reproduisait l'énoncé de l'arrêté royal précédemment d'application : il demandait que le responsable du traitement mentionne la base légale ou réglementaire *précise*. Ce projet fut soumis pour avis à la Commission de la protection de la vie privée qui estima qu'une telle exigence risquait d'imposer une obligation trop lourde et, partant, d'ouvrir la porte aux abus[3]. « En conséquence, le texte de l'arrêté a été modifié et l'indication "précise" supprimée. On avoue que si l'on doit admettre comme trop lourd le fait pour un responsable de connaître précisément la base légale qui l'autorise à traiter des données en prin-

---

1. C. DE TERWANGNE, « La nouvelle loi belge de protection des données à caractère personnel », *in* P. TABATONI (dir.), *La protection de la vie privée dans la société d'information. Cahier des Sciences morales et politiques*, Paris, PUF, 2002, disponible sur le site de l'Académie des Sciences morales et politiques, http://www.asmp.fr/travaux/gpw_internetvieprivee.htm, pp. 111 et 112.
2. « Le fait que, parmi les données visées par cette disposition, certaines n'ont pas de caractère confidentiel, ne semble pas être pris en compte pour l'application de la disposition. Ainsi, dans le cas de la collecte d'informations révélant l'appartenance politique d'élus (personnes ayant donc fait campagne et manifestement rendu publiques ces données, ce qui autorise leur traitement), les fonctionnaires ou autres utilisant ces informations doivent être tenus à un devoir de confidentialité. Le fonctionnaire communal qui présente sur le site Internet de la commune la composition des organes, indiquant le nom des élus et leur parti politique, ou les personnes qui rédigent les comptes rendus des séances des assemblées législatives en mentionnant l'appartenance politique des intervenants, doivent être tenus statutairement ou contractuellement à un devoir de confidentialité à l'égard de ces données. La solution ne soulèvera sans doute guère de problèmes dans la pratique, personne ne songeant à s'insurger contre un fonctionnaire qui aurait, en dehors de ses tâches, révélé à autrui le parti d'un élu. Mais tout de même, imposer le secret concernant des données de notoriété publique heurte la logique. La lecture correcte de la disposition doit sans doute, en conséquence, conduire à comprendre que la disposition ne confère pas elle-même aux données visées aux articles 6 à 8 de la loi un caractère confidentiel mais, là où ce caractère existe ou lorsque la personne concernée n'entend pas rendre les données publiques, l'arrêté royal prescrit d'imposer le secret aux personnes accédant aux données. » (C. DE TERWANGNE et S. LOUVEAUX, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.*, 2001, p. 459.)
3. Avis 8/99 du 8 mars 1999 : « La Commission fait remarquer que l'obligation de mentionner la base légale « précise » peut comporter certains risques. Si cette disposition devait imposer une obligation trop lourde et s'il devait s'avérer impossible d'agir conformément à la loi, cette disposition ouvrirait la porte aux abus. »

cipe interdites, il est à craindre pour l'efficacité même du système protecteur. La Commission conçoit donc que des personnes traitent des données sensibles, médicales ou judiciaires sans savoir avec précision sur quoi elles s'autorisent pour contourner l'interdiction de principe. À notre sens, c'est plutôt dans de telles circonstances que la porte risque d'être ouverte aux abus »[1] ;

- Enfin, lorsque le traitement de données sensibles au sens strict ou relatives à la santé se fonde exclusivement sur le consentement par écrit de la personne concernée, le responsable du traitement doit informer la personne concernée des motifs pour lesquels ces données sont traitées ainsi que communiquer la liste des catégories de personnes ayant accès aux données.

6. Les droits de la personne concernée

Les droits octroyés à la personne concernée le sont afin de permettre à celle-ci d'exercer pleinement son autodétermination informationnelle. Ils visent en premier lieu à assurer la transparence des traitements de données aux yeux de la personne concernée. L'autodétermination informationnelle implique en effet au minimum, ainsi qu'on l'a dit[2], d'avoir connaissance du sort réservé à ses données. Cette transparence, d'initiative ou sur demande, doit permettre à la personne concernée non seulement d'avoir connaissance, mais aussi de contrôler ce qui est fait avec ses données, de vérifier le respect des règles, de traquer les abus ou les illégalités, de corriger les erreurs.

Le Conseil d'État a d'ailleurs défini le droit d'accès, dont il sera question au point 6.2. ci-dessous, comme « un droit de contrôle [pour le citoyen] sur les données concernant sa personne qui ont été rassemblées dans un fichier »[3].

Il est à noter qu'un recours juridictionnel spécifique a été mis en place par la loi du 8 décembre 1992[4]. Une possibilité d'action est ouverte auprès du président du tribunal de première instance siégeant comme en référé, afin de lui soumettre toute demande concernant l'exercice des principaux droits garantis à la personne concernée (droit d'accès, droit de rectification et droit d'opposition – voy. *infra*).

Un recours devant les juridictions pénales est également envisageable en cas de non-respect des obligations liées au droit à l'information et au droit d'accès, étant

1. C. DE TERWANGNE et S. LOUVEAUX, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *op. cit.*, p. 459.
2. Voy. l'introduction du présent ouvrage.
3. C.E., 13 novembre 2006, n° 164.654, point 3.4.2 ; traduction libre.
4. Article 14 de la loi du 8 décembre 1992.

donné que ce non-respect est sanctionné pénalement[1]. De plus amples développements sont consacrés à ces deux types de recours dans le point ultérieur dédié aux voies de recours.

6.1. Le droit à l'information

Le traitement des données doit se faire dans la transparence, troisième grand principe de protection des données après le principe de finalité et celui de proportionnalité évoqués antérieurement. Il s'agit, dans un premier temps, pour le responsable du traitement, de fournir spontanément de l'information à la personne concernée à propos du traitement qui va être effectué avec les données la concernant. Ce droit pour l'un s'apparente donc à une obligation pour l'autre. Le droit à l'information est présenté en détail sous son aspect d'obligation de fournir des informations à la personne concernée dans le chapitre consacré aux obligations du responsable du traitement (voy. le point 7.1.2. *infra*).

6.2 Le droit d'accès

Le droit d'accès offre à la personne concernée une autre voie pour obtenir des informations sur les traitements effectués sur ses données. Cette voie n'offre toutefois pas les mêmes garanties que le devoir d'information pesant sur le responsable du traitement (voy. les points 6.1. *supra* et 7.1.2. *infra*), car elle exige une démarche de la part de la personne concernée, celle-ci devant au demeurant avoir déjà connaissance de l'identité du responsable du traitement.

Le non-respect du droit d'accès est pénalement sanctionné[2].

6.2.1. L'accès comme moyen de contrôle individuel

Le droit d'accès est fondamental pour la personne concernée afin qu'elle puisse procéder à diverses vérifications concernant les données à caractère personnel se rapportant à elle. Sur cette base, elle pourra prendre connaissance des données traitées et s'assurer que le traitement est conforme à la loi vie privée. De ce premier droit découle l'exercice d'autres droits tels que les droits de rectification, d'opposition et de recours.

1. Article 39, 4° et 5°, de la loi du 8 décembre 1992.
2. L'article 39, 5°, LVP punit d'une amende de cent francs à cent mille francs le responsable du traitement, son représentant en Belgique, son préposé ou mandataire, qui n'a pas donné communication, dans les quarante-cinq jours de la réception de la demande, des renseignements visés à l'article 10, § 1er.

Dans le même sens, la Cour de justice de l'Union européenne a considéré, dans un arrêt du 7 mai 2009 :

> « 49. Ce droit au respect de la vie privée implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont traitées de manière exacte et licite, c'est-à-dire, en particulier, que les données de base la concernant sont exactes et qu'elles sont adressées à des destinataires autorisés. Ainsi qu'il est énoncé au quarante et unième considérant de la directive, afin de pouvoir effectuer les vérifications nécessaires, la personne concernée doit disposer d'un droit d'accès aux données la concernant qui font l'objet d'un traitement.
>
> 50. À cet égard, l'article 12, sous a), de la directive prévoit un droit d'accès aux données de base ainsi qu'à l'information sur les destinataires ou les catégories de destinataires auxquels ces données sont communiquées.
>
> 51. Ce droit d'accès est nécessaire pour permettre à la personne concernée d'exercer les droits visés à l'article 12, sous b) et c), de la directive, à savoir, dans le cas où le traitement de ses données ne serait pas conforme à cette directive, celui d'obtenir que le responsable du traitement rectifie, efface ou verrouille ses données [sous b)] ou qu'il notifie aux tiers auxquels les données ont été communiquées ces rectification, effacement ou verrouillage, si cela ne s'avère pas impossible ou ne présuppose pas un effort disproportionné [sous c)].
>
> 52. Ce droit d'accès est également nécessaire pour permettre à la personne concernée d'exercer le droit d'opposition au traitement de ses données à caractère personnel visé à l'article 14 de la directive ou le droit de recours en cas de dommage subi prévu aux articles 22 et 23 de celle-ci »[1].

Ce moyen de contrôle individuel est différent du contrôle a priori exercé par la Commission de la protection de la vie privée, qu'il vient compléter. Ce contrôle a priori de la Commission s'exerce sur la base de l'obligation qui pèse sur les responsables de traitements de déclarer ceux-ci auprès de la Commission (voy., *infra*, le point 7.1.1.). Pour la Cour de cassation, par les articles de la loi vie privée instaurant le devoir de déclaration et le droit d'accès, « le législateur, d'une part, crée, par la déclaration du responsable du traitement, un contrôle *a priori*, au profit de la Commission de la protection de la vie privée, en vue de lui permettre de s'assurer de la conformité du traitement déclaré avec les principes énoncés par la loi, et, d'autre part, impose au responsable du traitement l'obligation, sanctionnée pénalement, de fournir à une personne physique qui le demande les informations dont la loi prévoit la communication »[2]. Il s'agit bien de deux voies de contrôle différentes, ne pouvant s'interchanger.

---

1. C.J.C.E., 7 mai 2009 (College van burgemeester en wethouders van Rotterdam c. m.e.e. Rijkeboer), aff. C-553/07.
2. Cass., 14 février 2013, C.11.0777.F.

6.2.2. Le droit d'obtenir des informations sur le traitement des données

a) Informations quant aux finalités du traitement, aux catégories de données traitées et de destinataires

En vertu de l'article 10, § 1er, alinéa 1er, a), de la LVP, chacun a le droit d'interroger tout responsable du traitement de données à caractère personnel pour savoir s'il détient ou non des données sur lui. Le responsable interrogé doit confirmer ou non s'il détient des données à propos de l'individu qui s'est adressé à lui et, si c'est le cas, il doit fournir des indications sur le sort réservé à ces données. Il doit à tout le moins éclairer la personne concernée sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées[1].

b) Informations quant aux destinataires présents et passés et devoir corrélatif de conserver les traces des communications des données

Le droit d'être informé des destinataires ou à tout le moins des catégories de destinataires à qui les données sont communiquées ainsi que du contenu des communications soulève la question de la portée dans le temps de ce type d'information. En effet, c'est souvent parce que l'on s'est rendu compte de quelque chose de douteux ou parce que l'on souhaite savoir à quelle source des personnes ont obtenu des informations, que l'on exerce son droit d'accès pour découvrir les personnes à qui les données ont été transmises. Il est donc important de savoir si le droit d'accès prévu par la loi couvre ces informations relatives à des faits passés ou ne vaut que pour le présent.

L'accès aux données sur les destinataires est aujourd'hui, dans un monde numérisé, lié à la question de l'accès aux *log files* ou journaux d'événements[2]. Ces derniers sont des fichiers qui relèvent un certain nombre de renseignements sur toutes les transactions gérées par le serveur. C'est donc à partir de ces journaux et des traces digitales qu'ils conservent que l'on peut identifier les accès qui se sont produits. L'accès aux données sur les destinataires se heurte directement aux pratiques d'effacement de telles informations au terme d'un certain délai.

Saisie d'une affaire mettant en cause un citoyen néerlandais désireux de connaître les personnes à qui ses données détenues par la commune avaient été communiquées, mais qui s'était heurté à une impossibilité d'être éclairé au-delà d'un an en raison de l'effacement de ce type de données, la Cour de justice de l'Union européenne[3] a affirmé que le sens même du droit d'accès dans toutes ses compo-

1. Article 10, § 1er, alinéa 1er, littera a, LVP.
2. Voir J. Herveg, «L'Accès du patient aux log files de son dossier informatisé », *Droit de la consommation*, 2011, p. 34-55.
3. C.J.C.E., 7 mai 2009 (College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer), C-553/07. Voy. C. GAYREL, « Chronique de jurisprudence en droit des technologies de l'information (2009-2011). Libertés et société de l'information. Cour de Justice de l'Union européenne, Tribunal de Première Instance et Tribunal de la Fonction publique européenne », *R.D.T.I.*, nos 48 et 49, 2012, pp. 95 et 96.

santes est de permettre aux individus de prendre connaissance du sort réservé à leurs données et de procéder à des vérifications des opérations effectuées sur elles, afin d'être à même d'exercer leurs autres droits prévus par la directive. En conséquence, pour la Cour, il est impératif que l'accès ne soit pas réduit au présent, mais couvre également le passé.

Il ne s'agit pas pour autant de permettre de remonter sans limites dans le temps, ce qui induirait une obligation corrélative pour les responsables de conserver indéfiniment les informations relatives aux actions réalisées avec les données, en l'occurrence aux communications des données. La fixation d'un délai de conservation légitime varie en fonction de paramètres identifiés par la Cour et doit être tempérée par l'intervention du critère de proportionnalité. Les paramètres à prendre en considération sont les suivants : la durée de conservation des données à caractère personnel « de base » ou « principales », celles qui font l'objet du traitement et dont les données relatives aux destinataires peuvent être considérées comme « accessoires » (en cas de très longue durée de conservation des données principales, l'intérêt de l'accès peut s'estomper au fil du temps, mais la durée de conservation des traces des communications doit tout de même demeurer dans un juste rapport de proportionnalité avec la durée de conservation des données principales), les délais de recours, la nature plus ou moins sensible des données principales, le nombre des destinataires et la fréquence des communications[1].

> « L'arrêt *Rijkeboer* présente un enseignement concret pour les responsables de traitement. Ils savent à l'avenir que découle de la directive (et dès lors des lois nationales qui l'ont transposée) l'obligation de veiller à la conservation des traces des communications et accès aux données accordés à des tiers pendant à tout le moins une durée raisonnable, afin de permettre aux personnes concernées d'être informées, à leur demande, de ces transmissions de leurs données et de pouvoir en contrôler la licéité »[2].

6.2.3. L'accès aux données à caractère personnel traitées

Aux termes de l'article 10, § 1er, alinéa 1er, b), de la LVP, la personne concernée qui apporte la preuve de son identité a le droit d'obtenir du responsable du traitement la communication, sous une forme intelligible, des données faisant l'objet du traitement.

Dès qu'il est sollicité par une personne concernée, le responsable du traitement doit donc communiquer sous une forme intelligible les données à caractère personnel

1. Voy. les paragraphes 58 et 59 et 63 de l'arrêt et leur commentaire dans C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », note sous C.J.U.E, 7 mai 2009, *R.D.T.I.*, 2011, n° 43, pp. 65 à 81.
2. C. DE TERWANGNE, « L'étendue dans le temps du droit d'accès aux informations sur les destinataires de données à caractère personnel », *op. cit.*

traitées. Il ne s'agit plus d'une information sur le traitement des données, mais de la communication bien concrète des données en cause. C'est l'ensemble des données traitées qui doivent être communiquées, tant les données objectives que les données subjectives (p. ex., avis ou opinions sur une personne).

L'exigence que les données soient communiquées sous une forme intelligible implique que la forme des données doit permettre à un individu ordinaire de saisir la portée de l'information transmise. Ainsi, si un code ou un profil particulier est attribué à la personne concernée (par une banque qui évalue sa valeur de crédit, par exemple, ou à l'issue de tests d'embauche), celle-ci doit être mise en mesure de comprendre la signification du code ou du profil.

On ne peut par ailleurs prétendre, ainsi que l'a fait la Cour d'appel de Liège dans une affaire mettant en cause un administré face à la Communauté française, qu'une réponse adéquate a été apportée à une demande formulée sur la base du droit d'accès par le seul fait d'avoir honoré la formalité de déclaration du traitement auprès de la Commission de la protection de la vie privée (voy., *infra*, point 7.1.1. pour cette formalité de déclaration). La cour d'appel avait constaté que la déclaration du traitement effectuée par la Communauté française auprès de la Commission de la protection de la vie privée faisait apparaître notamment les catégories de données à caractère personnel traitées. Comme cette déclaration avait été communiquée au conseil du demandeur lors des débats devant le premier juge, la Cour d'appel s'autorisa à conclure que, « dès la procédure devant le premier juge, [le demandeur] avait obtenu, par ce biais, les informations réclamées par [sa lettre] [...] que, aux termes de l'article 10 de la loi du 8 décembre 1992, il était en droit d'obtenir »[1]. L'arrêt en question a été cassé par la Cour de cassation refusant de suivre pareil raisonnement[2].

Pour la Cour de cassation, seule la transmission des informations portant sur les données à caractère personnel faisant l'objet du traitement, adressée par le responsable du traitement à la personne physique qui les demande, répond au devoir d'information mis à charge du responsable du traitement vis-à-vis de la personne concernée[3].

6.2.4. L'accès à l'information sur l'origine des données

L'article 10, § 1er, alinéa 1er, b), de la LVP garantit aussi à toute personne concernée le droit d'obtenir du responsable du traitement la communication, sous une forme intelligible, de toute information disponible sur l'origine des données.

1. Liège, 3 février 2009, cité par Cass., 14 février 2013, C.11.0777.F.
2. Cass., 14 février 2013, C.11.0777.F.
3. Cass., 14 février 2013, préc.

Inexistant en Belgique avant la transposition de la directive européenne en droit interne, cette obligation d'information sur l'origine des données, qui est logiquement d'application lorsque les données n'ont pas été recueillies directement auprès de la personne concernée, est d'un grand intérêt étant donné que c'est souvent la question de la source des informations qui préoccupe les personnes concernées (comment se fait-il que mes informations se retrouvent dans les mains de cette personne, qui les lui a fournies ?).

Par ailleurs, les renseignements sur l'origine des données permettent de vérifier la licéité de la communication ou de la collecte de celles-ci et, éventuellement, d'introduire un recours à l'encontre du premier détenteur des données (ce qui permet « d'arrêter l'hémorragie » si celui-ci diffuse illicitement les données en question).

Enfin, en cas de problèmes liés à la qualité des données et de nécessité de correction, il devient possible de faire effectuer ces corrections à la source, ce qui évite la propagation ultérieure d'erreurs.

6.2.5. L'accès à la logique qui sous-tend le traitement des données

Lorsqu'une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, cette personne doit pouvoir obtenir du responsable du traitement la connaissance de la logique qui sous-tend le traitement automatisé en question[1].

Le but de ce droit d'accéder à la logique d'un traitement consiste à permettre aux personnes concernées de contrôler les fondements de décisions prises à leur encontre, impliquant le traitement de leurs données.

Dans le contexte technique actuel, ce droit d'avoir connaissance de la logique (le raisonnement, les critères ou le programme d'ordinateur) qui sous-tend tout traitement automatisé des données présente un grand intérêt, notamment face au déploiement exponentiel du phénomène de profilage.

Cette garantie consacrée par l'article 12 de la directive 95/46 a un potentiel d'application qui a fait dire à M. Rotenberg (de l'EPIC – Electronic Privacy Information Center – Washington) qui l'évoquait : « There is a giant sleeping in the EU directive. That is the right to know the logic of a data processing »[2].

---

1. Article 10, § 1er, alinéa 1er, c), de la loi du 8 décembre 1992.
2. M. Rotenberg lors de l' *International Conference on Privacy and Data Protection « Re-inventing Data Protection ? »*, Bruxelles, 12 et 13 octobre 2007.

6.2.6. Modalités d'exercice du droit d'accès

La procédure d'accès à ses données a été considérablement assouplie pour la personne concernée par rapport à ce qui existait avant la modification de la loi vie privée en 1998.

Pour exercer son droit d'accès, la personne concernée doit adresser une demande au responsable du traitement. La demande doit être datée et signée par la personne concernée qui soit la remet sur place, soit l'envoie par la poste (l'exigence d'un pli recommandé a été supprimée) ou par tout moyen de télécommunication[1].

Ceci implique que les demandes pourront, par exemple, être introduites par courrier électronique, mais seulement accompagnées d'une signature électronique considérée comme juridiquement équivalente à la signature manuscrite.

Quant aux demandes effectuées par téléphone, elles soulèvent le problème de la preuve de l'identité des demandeurs. Comment s'assurer en effet que la personne qui téléphone est bien celle qu'elle annonce ? Il ne s'agit pas d'aller communiquer des informations bancaires ou médicales, par exemple, à un tiers curieux ou malhonnête qui se fait passer pour la personne concernée. L'article 10 de la loi exige d'ailleurs que la personne concernée « apporte la preuve de son identité ». Pour l'arrêté royal, le droit d'accès est reconnu à « toute personne justifiant de son identité », la version flamande étant plus proche de la loi : « eenieder die zijn identiteit bewijst ». Il est clair que décliner son identité par téléphone ne revient pas à « apporter la preuve » ni à « justifier de » son identité. Dans le cas des demandes d'accès par la voie téléphonique, on ne pourra donc sans doute pas faire l'économie de l'envoi de la photocopie de la carte d'identité ou d'un autre document identifiant.

La demande devra être adressée soit au responsable du traitement ou à son représentant en Belgique ou à un de ses mandataires ou préposés, soit au sous-traitant qui communiquera la demande au responsable.

Il est à noter que l'arrêté royal qui fixait le montant de la somme que le demandeur pouvait se voir réclamer lors d'une demande d'accès (soit 100 francs belges) a été abrogé. Aucun texte n'est à ce jour venu remplacer cette disposition. On pourrait, dès lors, s'interroger sur la légalité de conditionner l'accès aux données au paiement des frais de gestion de la demande : si cette condition peut se justifier[2], le prix

1. Article 32 de l'arrêté royal du 13 février 2001.
2. En ce qui concerne le droit de rectification, l'article 12 de la loi mentionne explicitement que ce droit doit s'exercer « sans frais ». On pourrait donc raisonner *a contrario* pour admettre l'exigence d'un paiement pour l'exercice du droit d'accès, la loi ne précisant pas pour celui-là qu'il s'exerce « sans frais ».

demandé ne pourra en tout cas être tel qu'il reviendrait à ôter toute efficacité au droit[1].

Le responsable du traitement doit répondre sans délai et au plus tard dans les quarante-cinq jours de la réception de la demande[2].

6.2.7. Accès indirect

En deux circonstances, la loi a prévu une formule d'accès indirect de la personne concernée à ses données.

a) L'accès aux données relatives à la santé

L'accès d'une personne aux données à caractère personnel relatives à sa santé peut s'effectuer soit directement, soit par l'intermédiaire d'un professionnel des soins de santé[3] choisi par elle, si le responsable du traitement, voire elle-même, demande l'intervention d'un intermédiaire[4].

La loi n'impose aucune motivation particulière de la part du responsable du traitement pour justifier le refus d'accès direct et la demande d'intervention d'un intermédiaire.

Pour des données relatives à la santé, on peut concevoir, si cela s'impose pour des raisons liées à l'état médical ou psychique de la personne concernée, que le professionnel des soins de santé présente l'information de manière « adoucie » au patient, ou accompagnée d'informations complémentaires éclairantes ou d'explications pour comprendre la portée des termes médicaux utilisés.

Par ailleurs, lorsque les données relatives à la santé de la personne concernée sont traitées aux fins de recherches médico-scientifiques, la communication peut être différée au plus tard jusqu'à l'achèvement des recherches. Il s'agit bien d'un droit différé et non pas d'une extinction du droit. Cela ne peut toutefois se faire qu'à certaines conditions :

- il doit être manifeste qu'il n'existe aucun risque qu'il soit porté atteinte à la vie privée de cette personne ;

---

1. A noter, à titre d'exemple, que l'article 9 de la loi relative aux droits du patient habilite le Roi à fixer le prix maximum qui peut être demandé au patient pour la copie de son dossier médical. Sur la base de cette habilitation, l'arrêté royal du 2 février 2007 fixant le montant maximal par page copiée pouvant être demandé au patient dans le cadre de l'exercice du droit d'obtenir une copie du dossier de patient le concernant a établi ce prix maximum à 0,10 € par page et 5,00 € par image médicale.
2. Article 10, § 1er, alinéa 3, LVP.
3. La loi n'indique pas ce qu'il faut entendre par « professionnel des soins de santé ». Sur ce point, voy. TH. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution », *op. cit.*, note 135.
4. Article 10, § 2, LVP.

- les données ne peuvent pas être utilisées pour prendre des mesures à l'égard d'une personne concernée individuelle ; et
- la communication des données non différée aux personnes concernées doit être susceptible de nuire gravement auxdites recherches[1].

Dans ce cas, la personne concernée doit avoir préalablement donné son autorisation écrite au responsable du traitement que les données à caractère personnel la concernant peuvent être traitées à des fins médico-scientifiques et que la communication de ces données peut dès lors être différée[2].

b) L'accès aux données détenues par les autorités de surveillance et de police : une exception officieuse ou l'absence d'accès

Pour les données traitées à des fins de sûreté de l'État, de sécurité publique, de défense nationale, de prévention ou de répression des infractions[3], il s'agit de trouver un juste équilibre entre les droits des personnes concernées et les nécessités tout aussi légitimes de la recherche ou de la poursuite des infractions, ainsi que de la prévention des atteintes à la sûreté de l'État et la sécurité publique.

Pour ce type de données, c'est un accès officiellement indirect qui est mis en place[4]. L'article 13 de la loi du 8 décembre 1992 stipule en effet que, *pour exercer son droit d'accès* à l'égard de ces données, l'intéressé doit s'adresser à la Commission de la protection de la vie privée[5]. Cette disposition laisse donc penser qu'il y aurait un réel exercice du droit d'accès, mais par l'intermédiaire de la Commission (comme pour les données relatives à la santé : la personne concernée reçoit *in fine* communication d'informations, éventuellement expurgées ou filtrées par l'intermédiaire).

Or, une fois effectuées les vérifications utiles par la Commission qui aura fait éventuellement procéder aux modifications nécessaires, la seule information communiquée au demandeur d'accès est qu'« il a été procédé aux vérifications ». Aucune autre donnée se rapportant à elle ne peut être transmise à la personne concernée[6]. De fait, celle-ci délègue entièrement son droit d'accès à la Commission de la protection de la vie privée et n'exerce plus aucun droit elle-même.

---

1. Article 10, § 2, alinéa 3, LVP.
2. Article 10, § 2, alinéa 4, LVP.
3. Plus précisément, les données traitées par les institutions visées à l'article 3, §§ 4, 5 et 6, de la loi du 8 décembre 1992.
4. Sur cet accès indirect, voy. B. HAVELANGE et Y. POULLET, « Secret d'État et vie privée : ou comment concilier l'inconciliable ? », *in Droit des technologies de l'information. Regards prospectifs*, coll. Cahiers du CRID, n° 16, Bruxelles, Bruylant, 1999, pp. 248 et s., spéc. pp. 257 à 260.
5. Il faut apporter la preuve de son identité et demander à la Commission de la protection de la vie privée d'effectuer la démarche d'accès, en se conformant aux prescriptions contenues à l'article 37 de l'arrêté royal du 13 février 2001. Sur l'ensemble de ces prescriptions et les modalités d'intervention de la Commission de la protection de la vie privée au titre de l'article 13 de la loi du 8 décembre 1992, voy. C. DE TERWANGNE et S. LOUVEAUX, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.*, 2001, pp. 462 et s.
6. L'article 46 de l'arrêté royal du 13 février 2001 prévoit un régime plus souple en ce qui concerne le traitement de données à caractère personnel géré par un service de police en vue d'un contrôle d'identité. Dans ce cas, la Commission communique à la personne concernée que les vérifications nécessaires ont été effectuées et, le cas échéant, elle peut fournir à la personne concernée, après avis du service concerné, toute autre information qu'elle estime appropriée.

Cette formule d'un « accès indirect » systématique pour les données en question est critiquable. L'article 13 de la directive qui autorise une telle limitation au principe du droit d'accès direct ne le fait que s'il s'agit d'une mesure « nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention et la poursuite d'infractions pénales [...] ». Il n'est donc pas question de limitation automatique du droit d'accès[1].

6.3. Le droit de rectification et d'effacement

6.3.1. Le droit

Toute personne concernée peut, sans frais, faire rectifier les données à caractère personnel inexactes qui se rapportent à elle et faire effacer ou interdire d'utilisation les données incomplètes ou non pertinentes au regard de la finalité du traitement ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée[2].

Dans le mois qui suit l'introduction de la demande de rectification ou d'effacement, le responsable du traitement communique à la personne concernée les rectifications ou effacements des données qu'il a effectués.

Dès la réception de la demande tendant à faire rectifier, supprimer ou interdire d'utiliser ou de divulguer des données à caractère personnel, et jusqu'à ce qu'une décision soit coulée en force de chose jugée, le responsable du traitement doit indiquer clairement, lors de toute communication d'une donnée à caractère personnel, que celle-ci est contestée[3].

6.3.2. Les modalités d'exercice du droit de rectification

Les demandes de rectification, de suppression et d'interdiction de traitement des données fondées sur l'article 12 de la loi se font selon la même procédure et auprès des mêmes personnes que ce qui est prévu pour l'exercice du droit d'accès.

6.3.3. Le droit de suite

Si des données inexactes, incomplètes ou non pertinentes ont été transmises à des tiers ou au public, le responsable doit, dans le mois qui suit l'introduction d'une requête en rectification portant sur ces données, communiquer les corrections ou effacements à effectuer aux personnes à qui ces données ont été communiquées.

---

1. Voy. Y. POULLET et B. HAVELANGE, *op. cit.*, pp. 233 et s.
2. Article 12, § 1er, alinéas 1er et 5, de la loi du 8 décembre 1992.
3. Article 15 de la loi du 8 décembre 1992.

Le responsable est cependant libéré de cette obligation lorsqu'il n'a plus connaissance des destinataires de la communication ou lorsque la notification paraît impossible ou implique des efforts disproportionnés[1].

6.4. Le droit d'opposition

6.4.1. Le droit

En vertu de l'article 12, § 1er, alinéas 2 et 3, de la LVP, toute personne a le droit de s'opposer à ce que les données la concernant fassent l'objet d'un traitement, pourvu qu'elle invoque des raisons sérieuses et légitimes tenant à sa situation particulière.

Le droit d'opposition n'est cependant pas reconnu pour les traitements nécessaires à la conclusion ou à l'exécution d'un contrat. De même, lorsque le traitement est nécessaire au respect d'une obligation légale ou réglementaire, les personnes concernées ne peuvent s'opposer au traitement. Il en va de même en matière de journalisme ou d'expression artistique ou littéraire (*Cfr.* supra)

Lorsque les données sont collectées à des fins de *direct marketing*, la personne concernée peut s'opposer gratuitement et sans aucune justification au traitement projeté de données à caractère personnel la concernant.

En cas d'opposition, le traitement mis en œuvre ne peut plus porter sur les données en cause.

Ce droit se justifie particulièrement lorsque le traitement des données ne repose pas sur le consentement des personnes concernées. Celles-ci, qui n'ont pu exprimer leur point de vue à l'entame du traitement, retrouvent par le biais de ce droit la possibilité de faire valoir leurs arguments auprès du responsable du traitement pour le convaincre de renoncer à traiter leurs données. Ce droit est particulièrement important dans les hypothèses où le responsable a effectué lui-même, *a priori*, la mise en balance des intérêts en présence et a estimé que le résultat était équilibré et qu'il pouvait légitimement traiter les données. Grâce au droit d'opposition, la personne concernée retrouve l'occasion de contester le résultat de la mise en balance, à tout le moins dans son cas.

En cas d'opposition au traitement de données à caractère personnel par la personne concernée, le responsable du traitement communique à cette dernière, dans le mois qui suit l'introduction de sa demande, quelle suite il a donnée à sa requête[2].

1. Article 12, § 3, de la loi du 8 décembre 1992.
2. Article 12, § 3, alinéa 2, de la loi du 8 décembre 1992

Dès la réception de la demande tendant à faire supprimer ou interdire d'utiliser ou de divulguer des données à caractère personnel, et jusqu'à ce qu'une décision soit coulée en force de chose jugée, le responsable du traitement doit indiquer clairement, lors de toute communication d'une donnée à caractère personnel, que celle-ci est contestée[1].

6.4.2. L'exercice du droit d'opposition

Les articles 34 et 35 de l'arrêté royal du 13 février 2001 établissent les modalités d'information sur le droit d'opposition. La loi prévoit en effet une obligation pour le responsable du traitement d'informer la personne concernée de son droit de s'opposer sur demande et gratuitement au traitement de ses données envisagé à des fins de *direct marketing* (art. 9, § 1er, e), et § 2, e) ; voy., *infra*, le point sur le devoir d'information). L'arrêté royal précise les modalités d'exercice de ce droit d'opposition.

Trois situations sont prévues par l'arrêté royal.

- La première vise celle où les données à caractère personnel sont collectées par écrit auprès de la personne concernée (p. ex., formulaire ou coupon-réponse à remplir). Dans ce cas, la personne concernée doit pouvoir exercer son droit d'opposition sur le document dans lequel elle communique les données à caractère personnel qui la concernent (p. ex., case à cocher).
- La deuxième situation vise les cas où les données sont obtenues auprès de la personne concernée autrement que par écrit (téléphone ou carte à puce, par exemple). Dans ces cas, le responsable du traitement doit prendre contact avec la personne concernée afin de lui demander si elle souhaite exercer son droit d'opposition au traitement des données à des fins de *direct marketing*. Cette prise de contact doit se faire soit sur un document permettant à la personne concernée d'exercer son droit d'opposition, soit par tout autre moyen technique permettant de garder une preuve que la personne concernée a eu la possibilité d'exercer son droit.
- La troisième situation (art. 35) concerne les hypothèses où les données à caractère personnel ne sont pas obtenues auprès de la personne concernée. Dans ces cas, le responsable doit en principe prendre contact avec la personne concernée afin de lui communiquer les informations prévues à l'article 9, § 2, de la loi. Lors de cette information, la personne concernée doit pouvoir marquer son opposition sur le document lui procurant cette information. Précisons que le responsable du traitement qui est dispensé de cette formalité d'information (notamment parce que l'information se révèle impossible ou implique des efforts disproportionnés) est également dispensé de cette obligation.

1. Article 15 de la loi du 8 décembre 1992.

6.4.3. Le droit de suite

Si des données ayant fait l'objet d'une opposition ont été transmises à des tiers ou au public, le responsable doit, dans le mois qui suit l'introduction d'une requête en opposition portant sur ces données, communiquer les effacements à effectuer aux personnes à qui ces données ont été communiquées. Le responsable est cependant libéré de cette obligation lorsqu'il n'a plus connaissance des destinataires de la communication ou lorsque la notification paraît impossible ou implique des efforts disproportionnés[1].

6.5. Le droit de ne pas être soumis à une décision automatisée

L'homme ne doit pas être soumis à la machine. Au nom de la dignité humaine, il est inadmissible qu'une décision qui s'impose à un individu dépende des seules conclusions d'une machine.

À l'exemple de la directive 95/46 qui a très opportunément traduit cette conviction dans son article 15[2], l'article 12*bis* de la LVP *interdit qu'une décision individuelle* produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative soit prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité.

Ce principe est crucial aujourd'hui alors que la technique est de plus en plus souvent utilisée pour s'en remettre à un « ordinateur » et aux algorithmes qu'il applique pour décider du traitement à réserver à un individu (le considérer ou non comme fraudeur fiscal, ou comme cible de marketing, ou comme voyageur candidat terroriste...). Les décisions affectant de manière significative les individus (p. ex., la décision de refuser d'embaucher quelqu'un ; d'arrêter un individu à une frontière et, éventuellement, de lui refuser l'entrée dans un pays ; de le soumettre à une surveillance intrusive, etc.) sont de plus en plus souvent motivées « par le fait que l'ordinateur a dit non », alors même que les personnes « responsables » de la décision ne comprennent pas nécessairement le calcul ou raisonnement appliqué par la machine à un ensemble de données pour aboutir à la conclusion énoncée[3].

Une telle interdiction doit bien évidemment connaître des limitations ou exceptions là où cela se justifie en considération du contexte et des risques en jeu. Ainsi, dans le monde commercial, il est courant de recourir à des évaluations automatisées du pro-

---

1. Article 12, § 3, de la loi du 8 décembre 1992.
2. Voy. l'analyse de cette disposition par L. BYGRAVE, « Minding the machine : Article 15 of the EC Data Protection Directive and automated profiling », *C.L.S.R.*, 2001, vol. 17, pp. 17 à 24.
3. LRDP KANTOR LTD, en association avec CENTRE FOR PUBLIC REFORM, *Étude comparative sur les différentes approches des nouveaux défis en matière de protection de la vie privée, en particulier à la lumière des évolutions technologiques*, Rapport final, Note de synthèse, disponible sur http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_fr.pdf, janvier 2010, p. 2.

fil du consommateur lorsqu'il s'agit de contrats d'octroi de prêt ou de souscription d'une assurance. Le recours à la technique du profil déborde désormais largement ces contextes commerciaux restreints et se nourrit de quantités impressionnantes de données glanées de toutes parts. Il est également fait recours à un traitement purement automatisé pour décider de la réussite ou de l'échec à certains examens (comme pour l'examen théorique pour le permis de conduire ou des examens de concours administratifs).

L'article 12*bis* prévoit que l'interdiction de soumettre un individu à une décision entièrement automatisée ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Pour être admissibles, ces exceptions doivent toutefois être accompagnées de mesures garantissant la sauvegarde de la dignité de l'homme face à la machine, c'est-à-dire la sauvegarde des intérêts légitimes de l'intéressé en prévoyant à tout le moins le droit pour l'intéressé de faire valoir *utilement* son point de vue. Les traitements effectués par les organismes de crédit et assurances évoqués ci-dessus, ne sont donc admissibles qu'à la condition que ces traitements soient contrôlés *in fine* par une personne physique

7. Les obligations du responsable de traitement

7.1. Assurer la transparence du traitement de données

Après les principes de finalité et de proportionnalité, le troisième principe fondamental sur lequel repose la loi vie privée est celui de la transparence de tout traitement. La transparence a déjà été évoquée lors de la mention de l'obligation de loyauté (*cf. supra*). Au-delà de la loyauté du traitement des données à caractère personnel, la transparence prend deux formes : l'une à l'égard de la personne concernée et l'autre à l'égard de la société dans son ensemble.

À l'égard de l'individu intéressé, la transparence s'exerce par le biais de l'obligation d'informer celui-ci et par le devoir de répondre à ses demandes d'accès aux données conservées. Le droit d'accès a été présenté sous le point dédié aux droits de la personne concernée. Il est donc renvoyé à ce point pour ce qui le concerne. Il convient, par contre, ici d'apporter les développements appropriés sur l'obligation d'information spontanée des personnes concernées qui pèse sur le responsable du traitement (point 7.1.2. relatif au devoir d'information des personnes concernées).

Mais, dans un premier temps, on s'attachera à présenter l'obligation de déclaration du traitement de données auprès de la Commission de la protection de la vie privée

(point 7.1.1. relatif à l'obligation de déclaration du traitement). Cette obligation doit en effet être remplie chronologiquement avant d'informer les personnes concernées. C'est avant la mise en œuvre du traitement, c'est-à-dire avant la collecte des données ou avant une nouvelle utilisation de données déjà collectées et conservées, que le responsable du traitement est tenu d'effectuer la formalité de la déclaration du traitement qu'il envisage.

7.1.1. L'obligation de déclaration du traitement de données auprès de la Commission de la protection de la vie privée

L'obligation de déclarer le traitement de données à caractère personnel à la Commission de la protection de la vie privée préalablement à sa mise en œuvre est prévue à l'article 17 de la loi du 8 décembre 1992.

Cette obligation de déclaration s'impose pour tout traitement entièrement ou partiellement automatisé ou tout ensemble de tels traitements ayant une même finalité ou des finalités liées[1]. La formalité ne s'applique donc pas aux traitements de données manuels ni à ceux effectués sur microfiches (qui ne sont pas considérées comme des moyens automatisés de traitement)[2].

L'obligation de déclaration ne connaît que quelques exceptions prévues par l'arrêté royal du 13 février 2001 en ses articles 51 et suivants. On signale que, hormis ces exceptions, presque tous les responsables de traitement sont tenus de remplir cette formalité, tant ceux du secteur public que du secteur privé, tant les grandes entreprises que les individus isolés. Notamment les services de police, le SPF Finances, les avocats, les médecins... sont soumis à cette obligation de déclaration[3].

La Commission de la protection de la vie privée met à la disposition de tout intéressé un formulaire type (sur papier ou en ligne) permettant d'effectuer la déclaration. Une contribution financière est à verser à chaque déclaration.

Tous les renseignements transmis dans la déclaration sont repris dans un registre public. Ce registre peut être librement consulté par quiconque sur place, dans les locaux de la Commission, mais également – et c'est surtout là l'intérêt aujourd'hui – en ligne[4]. On peut demander à recevoir un extrait du registre.

---

1. La notion de « finalités liées » qui provient du texte de la directive 95/46 (art. 18, § 1er) a suscité de légitimes questionnements doctrinaux, étant donné que cette notion nouvelle n'a fait l'objet d'aucune véritable élucidation de la part du législateur européen et n'a été l'occasion que de quelques remarques non concluantes dans les travaux préparatoires de la loi belge. On retiendra, finalement, qu'il faut sans doute entendre par là les finalités compatibles entre elles qu'un même traitement poursuivrait, tandis que des finalités incompatibles entraîneraient qu'il faut envisager le traitement comme deux traitements différents, devant chacun faire l'objet d'une déclaration distincte auprès de la Commission de la vie privée (Th. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, pp. 392 et 393).
2. Article 17, § 1er.
3. Voy. C. de Terwangne, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *op. cit.*, pp. 149 et s.
4. À l'adresse http://www.privacycommission.be/fr/registre-public.

Si cette étape peut paraître fastidieuse à certains, et particulièrement à certaines entreprises, elle n'en demeure pas moins importante pour, au moins, trois raisons.

- Porter l'existence du traitement à la connaissance du public via le registre public accessible sur le site Internet de la Commission de la protection de la vie privée. Cela permet également à la personne concernée potentielle d'appréhender ledit traitement à l'instar de ce qu'elle ferait avec une loi. Cela lui permet donc de pouvoir évaluer la portée d'un traitement, les mesures de sécurité qui l'entourent, etc. L'attention est cependant attirée sur le fait que la déclaration ne dispense pas le responsable de traitement de fournir une information à la personne concernée.
- Obliger le responsable du traitement à analyser son traitement en termes de finalités, de qualité des données, de sécurité, etc. Cela n'est pas négligeable, et ce, surtout pour de petites structures qui n'ont pas nécessairement un service juridique ou un délégué à la protection des données en leur sein. Une telle analyse peut donc se révéler utile pour éviter que la protection des données à caractère personnel ne soit négligée par manque de temps ou d'intérêt.
- Permettre à la Commission de la protection de la vie privée d'opérer un contrôle et, le cas échéant, d'interroger le responsable du traitement sur certaines ambiguïtés de sa déclaration. À condition, évidemment, qu'elle en ait les capacités logistiques et financières...

a) Contenu de la déclaration

La déclaration comporte une description des caractéristiques du traitement. Doivent y figurer notamment[1] :

- les finalités du traitement ;
- les catégories de données traitées (pas les données elles-mêmes), avec une description particulière des données visées aux articles 6, 7 et 8 de la loi (données sensibles, médicales et « judiciaires » – voy. *supra*) ;
- les catégories de destinataires à qui les données peuvent être fournies ;
- les garanties entourant la communication de données à des tiers ;
- les moyens par lesquels les personnes à propos desquelles des données sont traitées en seront informées ;
- les mesures prises pour faciliter l'exercice du droit d'accès ;
- les catégories de données destinées à être transmises à l'étranger et les pays de destination ;
- la période au-delà de laquelle les données ne peuvent plus être gardées, utilisées ou diffusées.

1. Voy. l'article 17 LVP pour le détail de ces éléments. Voy. également les formulaires préétablis par la Commission de la protection de la vie privée pour remplir la formalité de déclaration, disponibles sur son site.

b) Effets de la déclaration

La formalité de déclaration poursuit les objectifs énumérés à l'entame du présent point. Il ne s'agit pas d'une condition de mise en œuvre des traitements de données à caractère personnel[1]. Le responsable du traitement ne doit attendre aucun feu vert qui serait accordé par la Commission une fois analysé le contenu de la déclaration. Il peut démarrer son traitement aussitôt sa déclaration faite.

Au contraire, certains traitements de données requièrent une autorisation préalable délivrée par les comités sectoriels (voy. *infra*). Il en va, par exemple, ainsi pour la transmission de données à caractère personnel issues du registre national (tel le numéro national). C'est au sein du secteur public que l'autorisation d'un des comités sectoriels existants est requise préalablement à tout échange de données entre administrations ou services[2].

c) Exceptions à l'obligation de déclaration

Aux termes de l'article 17, § 8, de la LVP, le Roi peut exempter de la formalité de déclaration certaines catégories de traitements, lorsque, compte tenu des données traitées et de la finalité poursuivie, il n'y a manifestement pas de risque d'atteinte aux droits et libertés des personnes concernées. La loi stipule que l'arrêté royal en question doit préciser les finalités de traitement, les catégories de données traitées, les catégories de personnes concernées, les catégories de destinataires et la durée de conservation des données.

Le fait qu'un traitement se qualifie pour une exemption n'empêche pas que le responsable du traitement doit pouvoir fournir les informations reprises dans la déclaration à toute personne qui en fait la demande. De même, la Commission de la protection de la vie privée conserve son pouvoir d'exiger d'autres éléments d'information. L'intérêt du responsable du traitement d'être exempté de l'obligation de déclaration se trouve dès lors réduit étant donné que, dans tous les cas, il doit tenir les renseignements à la disposition de quiconque en fait la demande[3]. À l'expérience, on s'est toutefois rendu compte qu'il y avait de toute façon un intérêt interne à effectuer l'exercice d'identifier pour chaque traitement de données les renseignements contenus dans la déclaration (tels que la base légale du traitement, les finalités, les catégories de données contenues, les catégories de destinataires, la période de conservation des données, etc.). Cela permet de réaliser précisément en quoi

1. M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau et Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, p.152
2. Voy. la partie du présent ouvrage consacrée à la protection des données à caractère personnel dans le contexte de l'administration.
3. Voy. D. De Bot, *Verwerking van persoonsgegevens*, Antwerpen, Kluwer, 2001, pp. 293 et 294.

consistent les ressources informationnelles dont on dispose, et cela représente un instrument de gestion de ces ressources[1].

Les traitements de données à caractère personnel qui ne doivent pas faire l'objet d'une déclaration sont présentés ci-dessous. Chaque exemption est soumise à des conditions particulières (quant à la nature des données, quant aux destinataires ou quant à la durée de conservation des données) auxquelles il faut être attentif, car ces conditions ne sont pas systématiquement les mêmes d'un cas d'exemption à l'autre.

Les exemptions sont accordées pour les traitements ordinaires d'une entreprise ou d'une organisation (pour la gestion des salaires, du personnel, des actionnaires, de la clientèle et pour la comptabilité) et pour les traitements de données courants des fondations, associations et ASBL ainsi que des écoles et universités. Les traitements de données pour gérer les contacts et ceux générés par les contrôles d'accès sont aussi dispensés de déclaration. Enfin, une dispense est accordée pour les traitements dont la publicité est déjà assurée par ailleurs (registres de la population, registres publics, Banque-carrefour de la sécurité sociale).

- *Les traitements nécessaires à l'administration des salaires des personnes au service du ou travaillant pour le responsable du traitement*[2]

  Par « personnes au service du ou travaillant pour le responsable du traitement », il faut entendre tout intéressé effectuant des prestations pour le responsable du traitement, quel que soit son statut (travailleur salarié, indépendant, intérimaire, stagiaire, apprenti, élève, etc.)[3]. De toute évidence, il n'y a pas de risque d'atteinte à la vie privée. Le traitement doit cependant uniquement porter sur les données qui sont utilisées pour l'administration des salaires (données d'identification, données financières, composition de la famille...). Elles ne peuvent être communiquées qu'aux personnes qui y ont droit (p. ex., communication des fiches de paie à un secrétariat social).

- *Les traitements qui visent l'administration du personnel au service du ou travaillant pour le responsable du traitement*[4]

  Par « l'administration du personnel », il faut entendre des fonctions telles que la sélection et le recrutement, la formation, l'organisation de travail, des plans de carrière... des personnes au service du ou travaillant pour le compte du responsable du traitement. Le traitement de données à caractère personnel par un

1. C. DE TERWANGNE et S. LOUVEAUX, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *op. cit.*, p. 459.
2. Article 51 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
3. Rapport au Roi, *M.B.*, p. 7871.
4. Article 52 de l'arrêté royal.

bureau de sélection ne rentre pas dans cette exemption, étant donné que le traitement porte sur des données portant sur des personnes ne travaillant pas pour le compte du responsable du traitement[1].

Le traitement ne peut porter ni sur des données relatives à la santé de la personne concernée, ni sur des données sensibles ou judiciaires au sens des articles 6 à 8 de la loi, ni sur des données destinées à une évaluation de la personne concernée. Tout traitement qui comporte des données relatives à la santé, tels, par exemple, des tests psychologiques, devront dès lors faire l'objet d'une déclaration. Il en va de même pour tout traitement qui comporte des données d'évaluation (résultats de séminaires d'évaluation, etc.). Les données ne peuvent être conservées au-delà de la période nécessaire à l'administration du personnel et ne peuvent être communiquées à des tiers sauf dans le cadre de l'application d'une disposition légale ou réglementaire ou pour autant que cela soit indispensable à la réalisation des objectifs du traitement (p. ex., la communication du nom de la personne de contact vis-à-vis d'un client ou l'inscription d'un membre du personnel à une conférence).

– *Les traitements qui se rapportent à la comptabilité du responsable du traitement*[2]

Les données doivent se rapporter exclusivement à la comptabilité du responsable du traitement ; le traitement ne doit concerner que les personnes dont les données sont nécessaires à la comptabilité, et ces données ne peuvent être conservées au-delà de la période nécessaire à la finalité du traitement. Les données à caractère personnel traitées ne peuvent être communiquées à des tiers sauf dans le cadre de l'application d'une disposition légale ou réglementaire ou pour autant que la communication soit indispensable pour la comptabilité.

– *Les traitements qui visent l'administration d'actionnaires ou d'associés*[3]

Cette exemption vise les traitements relatifs à l'enregistrement des actionnaires et associés, à la gestion des bénéfices financiers, aux convocations à et procès-verbaux de réunions... Le traitement ne peut porter que sur des données nécessaires à cette administration et ne peut concerner que des personnes dont les données sont nécessaires à cette administration. L'exemption se limite donc à la gestion des actionnaires ou associés du responsable du traitement ou de sociétés appartenant à un même groupe. Les données ne peuvent être communiquées à des tiers sauf dans le cadre de l'application d'une disposition légale ou réglementaire.

1. Voy. le paragraphe précédent pour une description des personnes visées.
2. Article 53 de l'arrêté royal.
3. Article 54 de l'arrêté royal.

– *Les traitements qui visent la gestion de la clientèle ou des fournisseurs*[1]

Cette exemption vise tout traitement de données qui a pour objectif la gestion de la relation professionnelle entre le responsable du traitement et le client. Elle couvre le traitement de toute une série de données : données d'identification nécessaires, données financières, enregistrement et suivi des commandes... Le traitement ne peut cependant porter sur aucune donnée sensible ou judiciaire au sens des articles 6 et 8 de la loi ni sur des données relatives à la santé. Rappelons que les données relatives à la santé visent non seulement les données médicales proprement dites, mais également des données comme les résultats de tests psychologiques, les données portant sur l'état de la personne (handicap...). Ainsi, par exemple, un courtier en assurances pourrait être exempté de déclarer les traitements de données portant sur ses clients, pour autant que le traitement ne porte pas sur des données sensibles. Toutes les personnes qui ont une relation commerciale avec le responsable du traitement, que cette relation soit effective, ancienne ou potentielle, sont visées. Le terme client fait également référence aux clients des professions libérales telles que les comptables, agents de change, avocats...

Dans le cadre de l'exemption portant sur la gestion de la clientèle, personne ne peut être enregistré sur la base d'informations obtenues de tiers. Ceci implique que le traitement ne peut contenir des clients potentiels sur la base de données fournies par des tiers (p. ex., un client potentiel signalé par un autre client lors d'une action de parrainage). Cette interdiction ne vaut pas en ce qui concerne les traitements concernant les fournisseurs.

Le responsable du traitement qui veut bénéficier de cette exemption ne peut conserver les données au-delà de la période nécessaire à la gestion normale de l'entreprise et ne peut communiquer les données à des tiers, sauf dans le cadre de l'application d'une disposition légale ou réglementaire ou encore aux fins de la gestion normale de l'entreprise. Ainsi, un commerçant qui communique les données de ses clients à des sociétés de marketing sera tenu de déclarer le traitement qu'il effectue. Par contre, la communication par un commerçant à des fins de gestion normale de son entreprise ne nécessite pas de déclaration : communication des données par une agence de voyage à la compagnie aérienne lors de la réservation d'un voyage (cependant, si des données sensibles ou relatives à la santé de la personne sont communiquées, l'exemption de déclaration tombe : réservation d'un avion avec la mention repas kasher par exemple).

1. Article 55 de l'arrêté royal.

- *Les traitements effectués par une fondation, une association ou tout autre organisme sans but lucratif dans le cadre de leurs activités ordinaires*[1]

  Le traitement ne doit porter que sur l'administration des membres propres, des personnes avec qui le responsable du traitement entretient des contacts réguliers ou des bienfaiteurs de la fondation, de l'association ou de l'organisme. Sont, par exemple, visés ici les membres d'une association caritative, d'une ASBL...

  Dans le cadre du traitement, aucune personne ne peut être enregistrée sur la base d'informations obtenues de tiers, et les données ne peuvent être communiquées à des tiers sauf dans le cadre de l'application d'une disposition légale ou réglementaire. De plus, les données ne peuvent être conservées au-delà de la période nécessaire à l'administration des membres, des personnes de contact et des bienfaiteurs.

- *Les traitements indispensables à la communication effectués dans le seul but d'entrer en contact avec l'intéressé*[2]

  Cette exemption vise les fichiers contenant des données utilisées à des fins de communication (nom, adresse, entreprise, fonction, adresse électronique...). L'exemption est uniquement applicable aux traitements de données qui ne tombent pas sous l'application d'une autre disposition de l'arrêté. Les données ne peuvent être communiquées à des tiers ni conservées au-delà de la période nécessaire à la finalité du traitement. De tels traitements portent en général sur des données concernant toutes les personnes avec lesquelles le responsable du traitement souhaite nouer ou entretenir des relations, que celles-ci soient commerciales ou non.

- *Les traitements portant sur l'enregistrement de visiteurs effectué dans le cadre d'un contrôle d'accès*[3]

  Les traitements portant sur l'enregistrement de visiteurs effectué dans le cadre d'un contrôle d'accès sont également exemptés pour autant qu'ils portent uniquement sur un nombre limité de données : nom, adresse professionnelle du visiteur, identification de son employeur, identification de son véhicule, nom, section et fonction de la personne visitée et le jour et l'heure de la visite. Si d'autres données sont traitées, le traitement n'est pas exempté de la déclaration.

  Les données ne peuvent être utilisées que pour ce contrôle d'accès et ne peuvent être conservées que le temps nécessaire à cet effet (en principe, dès lors,

1. Article 56 de l'arrêté royal.
2. Article 57 de l'arrêté royal.
3. Article 58 de l'arrêté royal.

les données doivent être effacées une fois la visite terminée sauf en cas de vérifications effectuées dans le cadre de la politique de sécurité interne). Les données ne peuvent être communiquées à quiconque.

- *Les traitements par les établissements d'enseignement en vue de gérer leurs relations avec leurs élèves ou étudiants*[1]

  Cette exemption vise les traitements par des établissements d'enseignement en vue de gérer leurs relations avec leurs élèves ou étudiants potentiels, actuels ou futurs. Toutefois, le traitement ne peut porter sur des données obtenues de tiers et les données ne peuvent être communiquées à des tiers. Ainsi, le traitement de données à caractère personnel par une université qui constitue des listes d'élèves du secondaire dans le cadre d'un recrutement de nouveaux étudiants n'est pas couvert par l'exemption. De même la communication de données relatives aux étudiants à des sociétés de recrutement n'est pas couverte par l'exemption. Enfin, les données ne peuvent être conservées que durant le temps utile à la gestion de la relation avec l'élève ou l'étudiant.

- *Les traitements effectués par les communes conformément à la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité, conformément à la législation électorale, ainsi qu'aux dispositions légales relatives aux registres de l'état civil ; les traitements effectués par des autorités administratives si le traitement est soumis à des réglementations particulières adoptées par ou en vertu de la loi et réglementant l'accès aux données traitées, ainsi que leur utilisation et leur obtention*[2]

  Pour certains traitements effectués par les autorités administratives, tel le Registre national, il existe déjà une réglementation détaillée réglant, entre autres, l'accès aux données, leur utilisation et la communication à des tiers.

  Concernant l'article 61 de l'arrêté royal, le Conseil d'État a critiqué la formulation en termes trop généraux de l'exemption, qui ne garantit pas que chaque réglementation respecte les conditions d'exemption posées par la loi (les finalités du traitement, les catégories de données, de personnes concernées, de destinataires et la durée de conservation des données doivent être précisées dans chaque texte). Le Conseil d'État avait conclu : « La disposition doit, dès lors, être omise ou à tout le moins fondamentalement revue, de manière à désigner avec précision les réglementations concernées qui remplissent les conditions légales. » Par souci de pragmatisme[3], la disposition n'a toutefois été ni omise ni revue.

---

1. Article 59 de l'arrêté royal.
2. Articles 60 et 61 de l'arrêté royal.
3. Rapport au Roi, *M.B.*, p. 7871.

- *Les traitements de données personnelles gérées par les institutions de sécurité sociale visées dans la loi du 15 janvier 1990 relative à l'institution d'une Banque-carrefour de la sécurité sociale*[1]

  Une exemption est prévue pour les traitements de données personnelles gérées par les institutions de sécurité sociale visées dans la loi du 15 janvier 1990 relative à l'institution d'une Banque-carrefour de la sécurité sociale. Cette exemption vise à éviter un double emploi avec le propre système de déclaration de la Banque-carrefour[2]. En effet, dans le cadre de cette loi, l'article 46, alinéa 1er, 6°, prévoit que le Comité de surveillance de la Banque-carrefour doit tenir à jour un relevé des informations de l'article 17, § 3, de la loi du 8 décembre 1992, et ce, pour chaque traitement automatisé de données à caractère personnel effectué par une institution de sécurité sociale, ainsi qu'un relevé des communications de données à caractère personnel dans et hors du réseau. Au demeurant, toute institution de la sécurité sociale doit déclarer ses traitements au Comité de surveillance de la Banque-carrefour. Ces listes seront mises à la disposition de la Commission de la protection de la vie privée.

7.1.2. Le devoir d'information

a) Le principe

Une deuxième application du principe de transparence évoqué ci-dessus fait peser sur le responsable du traitement de données à caractère personnel une obligation d'information des personnes concernées par les données. Cette information doit être spontanée et ne survient donc pas à la suite d'une quelconque démarche effectuée par la personne concernée.

L'article 9 de la LVP prescrit ce qui suit :

> « § 1. Le responsable du traitement ou son représentant doit fournir à la personne concernée auprès de laquelle il obtient les données la concernant et au plus tard au moment où ces données sont obtenues, au moins les informations énumérées ci-dessous, sauf si la personne concernée en est déjà informée :
>
> a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;
>
> b) les finalités du traitement ;

1. Article 62 de l'arrêté royal.
2. Voy. la présentation de la Banque-carrefour de la sécurité sociale et les développements qui lui sont réservés dans la partie du présent ouvrage consacrée à la protection des données dans le secteur public.

c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de *direct marketing* ;

d) d'autres informations supplémentaires, notamment :
- les destinataires ou les catégories de destinataires des données,
- le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse,
- l'existence d'un droit d'accès et de rectification des données la concernant ;

sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ;

e) d'autres informations déterminées par le Roi en fonction du caractère spécifique du traitement, après avis de la commission de la protection de la vie privée.

§ 2. Lorsque les données n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne concernée en est déjà informée :

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;

b) les finalités du traitement ;

c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de *direct marketing* ; dans ce cas, la personne concernée doit être informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de *direct marketing* ;

d) d'autres informations supplémentaires, notamment :
- les catégories de données concernées ;
- les destinataires ou les catégories de destinataires ;
- l'existence d'un droit d'accès et de rectification des données la concernant ;

sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont traitées, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ;

e) d'autres informations déterminées par le Roi en fonction du caractère spécifique du traitement, après avis de la Commission de la protection de la vie privée.

Le responsable du traitement est dispensé de fournir les informations visées au présent paragraphe :

a) lorsque, en particulier pour un traitement aux fins de statistiques ou de recherche historique ou scientifique ou pour le dépistage motivé par la protection et la promotion de la santé publique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ;

b) lorsque l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance. »

Quand doit-on informer ?

Cette formalité d'information doit être accomplie soit au moment où l'on recueille des données à caractère personnel, lorsque celles-ci sont obtenues de la personne concernée elle-même, soit dès l'enregistrement ou, au plus tard, au moment de la première communication des données, lorsque les données sont obtenues de manière indirecte.

Le Tribunal correctionnel de Bruxelles a jugé, à l'occasion de l'affaire *Gaïa*[1], que l'ASBL, qui avait filmé des éleveurs de bestiaux en caméra cachée, n'avait pas tenu compte, entre autres, des articles 9, 16 et 17 de la loi du 8 décembre 1992. Elle n'avait donc pas respecté son devoir d'information des personnes filmées au moment des enregistrements. Le tribunal a estimé que le fait que les images aient été prises dans un lieu public n'avait aucune incidence.

1. Corr. Bruxelles (51e ch.), 14 janvier 2002, *A.M.*, 2002, p. 198.

Quelles informations faut-il fournir ?

Le responsable du traitement est tenu de fournir aux personnes concernées les informations suivantes :

- ses coordonnées (nom et adresse) ;
- les finalités (liées) du traitement ;
- l'existence du droit de s'opposer gratuitement au traitement envisagé à des fins de *direct marketing* (ce qui recouvre toutes démarches de promotion) ; cette information ne doit être fournie que si de telles finalités sont envisagées[1] ;
- les destinataires ou les catégories de destinataires des données (personnes à qui les données seront communiquées) ;
- l'existence d'un droit d'accès et de rectification des données ;
- le caractère obligatoire ou non des réponses ainsi que les conséquences d'un défaut éventuel de réponse (lorsque les données sont collectées auprès de la personne concernée) ; et
- les catégories de données (lorsque les données sont obtenues de source indirecte).

Les quatre derniers types d'information à fournir ne doivent pas être communiqués si, compte tenu des circonstances particulières dans lesquelles le traitement est effectué, cela n'est pas nécessaire pour assurer un traitement loyal des données. Les informations concernant les destinataires des données ne doivent pas être fournies si ces destinataires ne sont que des personnes internes au service de l'entreprise qui effectue la collecte des données, par exemple. Cette catégorie de destinataires entre en effet dans les attentes raisonnables des personnes concernées.

Rappelons que, pour certaines données telles que les informations sensibles, celles relatives à la santé ou à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté, des informations complémentaires doivent être données, ainsi que cela est prévu au chapitre III de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992[2].

Ainsi, le responsable du traitement doit ajouter aux informations fournies au titre de l'article 9 la *base légale ou réglementaire* autorisant le traitement de ces données particulières.

L'article 26 de l'arrêté royal impose une obligation supplémentaire d'information lorsque le traitement de données sensibles ou relatives à la santé se fonde exclusive-

1. TH. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, p. 389.
2. Voy. point 5.5.1., c), *supra*.

ment sur le consentement par écrit de la personne concernée. Dans ce cas, le responsable du traitement doit informer la personne concernée des *motifs* pour lesquels ces données sont traitées ainsi que communiquer la *liste des catégories de personnes ayant accès aux données*. Ces informations s'ajoutent, elles aussi, à celles qui doivent être fournies en vertu de l'article 9 de la loi. Rappelons que, parmi les informations déjà communiquées obligatoirement au titre de l'article 9, se trouvent les finalités du traitement. Qu'est-ce qui va distinguer dès lors les *motifs* (*redenen* en néerlandais) pour lesquels les données sont traitées des finalités poursuivies par le traitement ? Après avoir signalé aux personnes concernées pourquoi on souhaitait effectuer un traitement de données, on doit préciser pourquoi on est appelé à traiter des données sensibles ou médicales dans le cadre de ce traitement. En fait, si l'on présente des finalités larges du traitement, qui ne permettent pas de déduire la raison d'une utilisation de données sensibles ou médicales, l'information supplémentaire aura du sens. Ainsi, si un établissement scolaire propose un formulaire unique concernant toutes les informations sur l'enfant, annonçant une finalité globale d'inscription et d'insertion dans la vie de l'établissement, il conviendra alors d'ajouter, pour la collecte des informations en lien avec la religion, le motif d'organisation des cours de religion/morale ou d'offre de certains types de menus à la cantine scolaire[1].

Comment doit-on informer ?

Ni la loi de 1992 ni son arrêté d'exécution ne précisent la forme que doit prendre la démarche d'information. Celle-ci peut donc être adaptée aux circonstances. Cela peut se faire oralement, de manière informelle lors d'un entretien, par exemple, durant lequel le responsable du traitement communique les informations requises. Mais, la plupart du temps, l'information prendra une forme écrite, ne fût-ce que dans une perspective de preuve du respect de l'obligation légale (qui est sanctionnée pénalement). Cette forme écrite peut elle-même prendre plusieurs expressions : formule apposée au bas d'un formulaire à remplir, mentions apparaissant sur les pages d'un site Web, panneaux apposés dans les endroits placés sous vidéosurveillance, etc. Signalons qu'un pictogramme (p. ex., un dessin de caméra) seul ne suffit pas, étant donné qu'il faut indiquer les coordonnées du responsable et les finalités du traitement des données.

b) Exceptions

Cette obligation d'information connaît certaines exceptions.

Ces exceptions ne sont essentiellement valables que dans les hypothèses de collecte indirecte des données à caractère personnel, c'est-à-dire une collecte qui n'est pas effectuée directement auprès de la personne concernée.

1. C. DE TERWANGNE et S. LOUVEAUX, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.*, 2001, p. 459.

En fait, mis à part les cas d'exception au bénéfice des autorités de police, de renseignement et, dans certaines circonstances, des journalistes et de l'administration des finances, un responsable du traitement ne pourra jamais s'abstenir de fournir les informations prévues à l'article 9 quand il obtient les données directement de la personne concernée elle-même (lors d'un entretien, par exemple, ou par le biais d'un formulaire à remplir ou en cas de conservation des traces électroniques laissées lors d'une visite du site Internet). Ce n'est que dans l'hypothèse où cette personne a déjà connaissance des informations en question qu'il n'y aura plus lieu de les lui communiquer.

La personne est déjà informée

Le responsable du traitement est en effet dispensé d'informer la personne concernée si celle-ci a déjà connaissance des informations à fournir[1]. Précisons que cette première exception n'est valable qu'en présence de personnes déjà « informées » et non « raisonnablement supposées informées »[2].

L'information est impossible ou implique des efforts disproportionnés

Seulement dans les cas où les données ont été obtenues de source indirecte, les responsables des traitements de données sont dispensés de fournir les informations requises dans l'hypothèse où l'information des personnes concernées se révèle impossible ou implique des efforts disproportionnés[3].

Toutefois, le responsable doit justifier l'impossibilité dans la déclaration qu'il doit faire par ailleurs (voy., *supra,* point précédent) auprès de la Commission de la protection de la vie privée.

Si c'est une impossibilité matérielle à laquelle avait pensé le législateur initialement, une impossibilité fonctionnelle ou juridique peut aussi être soulevée. Ainsi, cette hypothèse d'exception « peut être invoquée par les avocats en faisant valoir que, plutôt qu'une impossibilité matérielle telle celle qu'avaient à l'esprit les rédacteurs de la loi (on ne dispose pas de données de contact relatives aux personnes concernées), l'exception doit jouer en vertu d'une impossibilité fonctionnelle (l'information contrarierait l'œuvre de l'avocat)[4] et légale (l'information emporterait violation du secret pro-

1. Article 9, § 1er et § 2, alinéa 1er, de la loi du 8 décembre 1992.
2. Voy. Y. POULLET et TH. LÉONARD, « La protection des données à caractère personnel en pleine (r)évolution », *op. cit.*, p. 386.
3. Article 9, § 2, alinéa 2, a), de la loi du 8 décembre 1992.
4. « C'est une préoccupation identique qui a amené les auteurs de la deuxième version de la loi à dispenser de la formalité d'information les personnes traitant des données aux fins de journalisme ou d'expression artistique et littéraire (afin de permettre l'exercice de la liberté d'expression). La défense des droits en justice est un intérêt qui peut, lui aussi, justifier, lors d'une mise en balance avec les intérêts protégés par la loi de 1992, des dérogations à l'égard des dispositions qui le compromettraient. » (C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *Cabinet d'avocats et technologies de l'information : balises et enjeux*, coll. Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005, p. 171, note 68).

fessionnel). [...] [L]'avocat peut donc dans certains cas, et notamment à l'égard de l'adversaire, se dispenser d'informer les personnes physiques à propos desquelles il recueille des données de manière indirecte [...] »[1].

L'exception pour les cas où l'information est impossible ou implique des efforts disproportionnés se révélera dans certains cas, en réalité, une obligation d'information différée dès lors que l'arrêté royal prévoit que le responsable de traitement « communique cette information, à la première prise de contact, avec la personne concernée »[2]. Cela est justifié par le fait que cette exception se base sur une impossibilité ou une disproportion de moyens à mettre en œuvre pour remplir l'obligation d'information. Cela implique donc que, dès l'instant où un tel obstacle disparaît, l'obligation doit être respectée. Si le responsable du traitement entre en contact pour d'autres raisons avec la personne concernée, il est prié de saisir l'occasion pour fournir les informations qu'il n'avait pas encore données jusque-là.

Si le responsable n'entre pas lui-même en contact avec la personne concernée, mais communique les données à un tiers, l'information devra alors être communiquée par ce tiers à la personne concernée. Ceci implique que, si le responsable du traitement communique les données à un tiers sans informer la personne concernée, il ne pourra être tenu responsable pour le défaut d'information à la personne concernée si le tiers à qui il communique les informations n'a pas respecté son devoir d'information lors de la première prise de contact.[3]

Cette situation vise plus particulièrement, mais non exclusivement, la prospection commerciale où des kyrielles de données à caractère personnel sont collectées par des entreprises spécialisées qui transmettent ensuite ces données à d'autres entreprises à des fins de *mailing*. Ce ne sont donc pas des finalités de recherches et de statistiques qui sont poursuivies (finalités qui bénéficient d'une exemption de l'obligation d'information, *cf.* ci-dessous). Dans ce cas, la deuxième entreprise n'a pas collecté les données directement auprès de la personne concernée et tombe en conséquence dans le champ d'application de l'article 9, § 2, alinéa 1er, de la loi. Elle pourra toutefois se prévaloir de l'exemption prévue à l'article 9, § 2, alinéa 2, de la loi vu le grand nombre de données et les efforts disproportionnés à mettre en œuvre pour informer les personnes concernées. Toutefois, lorsqu'elle entrera en contact avec chaque personne concernée lors d'un mailing, elle devra alors fournir à chacune les informations requises par l'article 9 de la loi. De même, si elle communique les données à un tiers, ce tiers devra informer les personnes concernées lors de la prise de contact avec elles.

1. C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *op. cit.*, p. 171.
2. Article 30 de l'arrêté royal du 13 février 2001.
3. Pour d'amples développements sur les questionnements que suscitent les conditions pour pouvoir bénéficier de la dispense du devoir d'information, voy. C. DE TERWANGNE et S. LOUVEAUX, *op. cit.*, pp. 460 et s.

L'enregistrement ou la communication des données est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance[1].

Pour cette dernière hypothèse, la directive a en fait énoncé de façon bien plus stricte l'exception au devoir d'information. La version belge permet au pouvoir exécutif de lever l'obligation d'information, au nom sans doute d'une quelconque efficacité, sans que cela fasse l'objet d'un débat dans une assemblée parlementaire. La directive n'admet, elle, de dispenser le responsable du traitement de fournir les informations requises aux personnes concernées que « si la législation prévoit expressément l'enregistrement ou la communication des données »[2]. Il faut donc que l'enregistrement ou la communication des données soit clairement prévu par la législation. S'en tenir aux termes de la loi belge hypothèque lourdement la transparence dans le secteur public et singulièrement dans l'administration. Tout fichage, toute communication de données, nécessaires, voire simplement utiles, pour répondre à une mission conférée en termes généraux par une norme législative ou réglementaire, peuvent se faire sans aucune mesure d'information des personnes concernées.

Conditions pour être exempté du devoir d'information

Outre les exceptions déjà prévues par la LVP, le chapitre IV de l'arrêté royal du 13 février 2001 établit les conditions pour être exempté de l'obligation d'information lorsque les données n'ont pas été obtenues directement auprès de la personne concernée[3].

L'article 28 de l'arrêté royal dispose que le responsable du traitement ultérieur à des fins historiques, statistiques ou scientifiques qui traite exclusivement des données codées est exempté de l'obligation d'information prévue à l'article 9, § 2, de la loi pour autant qu'il respecte les conditions de traitement prévues par l'arrêté[4]. Il y a lieu de déterminer précisément le champ d'application de cette exemption. Elle ne vise, en effet, que les cas où le responsable du traitement initial ou un tiers, qui n'ont pas obtenu les données directement auprès de la personne concernée, souhaitent ensuite traiter les données à des fins historiques, statistiques ou scientifiques. Il y a donc eu une information de la personne concernée au départ sur la finalité initiale, mais pas concernant cette finalité ultérieure. Cela suppose également que le traitement ultérieur ne soit pas compatible avec la finalité initiale car, sinon, une information sur une finalité secondaire ne serait pas nécessaire[5]. Donc, lorsqu'un responsable collecte des données pour des finalités particulières et décide ultérieurement de réali-

1. Article 9, § 2, alinéa 2, littera b, de la loi du 8 décembre 1992.
2. Article 11, § 2, de la directive 95/46.
3. Voy. les commentaires approfondis sur ces conditions *in* C. DE TERWANGNE et S. LOUVEAUX, *op. cit.*, pp. 460 et s.
4. Voy. *supra*.
5. Voy. C. DE TERWANGNE et S. LOUVEAUX, *op. cit.* ; M.-H. BOULANGER, C. DE TERWANGNE, TH. LÉONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, *op. cit.*, p. 146.

ser des statistiques à partir des données récoltées qu'il coderait pour ce faire, il ne doit pas informer la personne concernée, sauf s'il s'agit de données sensibles, médicales ou judiciaires.

L'article 29 prévoit qu'une autorité administrative chargée explicitement par la loi de rassembler et de coder les données est exemptée de l'obligation d'information lorsqu'elle agit en tant qu'organisation intermédiaire[1]. L'arrêté vise ici des organismes tels que la Banque-carrefour ou l'Institut National des Statistiques.

Enfin, l'article 31 prévoit que le responsable qui ne peut informer les personnes concernées parce que cette information est impossible ou requiert des efforts disproportionnés, doit justifier cette impossibilité auprès de la Commission, dans sa déclaration. La Commission devra publier la liste de ces responsables de traitement dans le registre public. Cette disposition vise à établir une certaine transparence des traitements pour lesquels aucune information n'a été fournie à la personne concernée.

7.2. Mettre les données à jour et assurer leur qualité

En vertu de l'article 4, § 2, de la LVP, il incombe au responsable du traitement de veiller à la qualité des données à caractère personnel traitées.

On a déjà vu dans les points précédents consacrés aux principes de finalité et de proportionnalité qu'aux termes de l'article 4, § 1er, 3°, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

Les données traitées doivent, en outre, être exactes et, si nécessaire, mises à jour.

Le responsable du traitement devra « faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8 »[2]. Il incombe donc au responsable du traitement de prendre toutes les mesures raisonnables pour que les données inexactes ou incomplètes, au regard des finalités poursuivies, soient effacées ou rectifiées. C'est une obligation de moyens et non de résultat qui est mise à charge du responsable.

1. Pour la définition et le régime applicable aux organisations intermédiaires, voy. *supra*.
2. Article 16, § 2, 1°, LVP.

On attire l'attention sur le fait qu'il ne peut être question de caractère exact ou inexact d'informations subjectives tels les avis ou opinions. On ne peut donc contester l'exactitude de telles informations. Toutefois, il importe que l'opinion émise s'appuie sur des données objectives dont l'éventuelle inexactitude pourra, elle, être mise en question.

À titre d'illustration de cette obligation de diligence concernant la qualité des données, il a été jugé en matière de crédit que le prêteur qui fournit des informations à l'U.P.C.[1] et à la Banque nationale est responsable d'un traitement de données ; c'est donc à lui « qu'il incombe de s'assurer que sont remplies toutes les conditions auxquelles la transmission du nom des débiteurs défaillants à l'U.P.C. et à la Banque nationale est subordonnée ». En transmettant une information inexacte, le prêteur a été jugé comme ayant commis une faute consistant en un manquement à l'obligation générale de prudence et diligence qui s'impose à tous[2].

Concernant les données à caractère personnel se rapportant à des enfants, le Groupe de l'article 29 a préconisé, dans ses documents de travail dédiés à cette question[3], qu'il soit tenu compte, pour l'obligation de mise à jour des données, du fait que l'enfant est en évolution constante. Les responsables du traitement des données doivent en conséquence être particulièrement attentifs à l'obligation de mise à jour des données à caractère personnel en présence de données se rapportant à des enfants[4].

7.3. Obligations de confidentialité et de sécurité

La confidentialité peut être définie comme « la sécurité visant à interdire l'accès à un système informatique »[5] ou comme « le caractère d'une information confidentielle »[6].

En réalité, l'article 16 de la LVP vise tant la confidentialité que la sécurité du traitement à deux niveaux, à savoir aux niveaux organisationnel et technique[7].

1. « Union professionnelle du crédit », association professionnelle représentative du secteur du crédit aux particuliers (www.upc-bvk.be).
2. Civ. Bruxelles (72e ch.), 15 octobre 2003, *J.T.*, 2004, pp. 140 et 141.
3. Groupe de l'article 29, document de travail 1/2008 du 18 février 2008 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles), *WP* 147 ; et Groupe de l'article 29, avis 2/2009 du 11 février 2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles), *WP* 160.
4. V. Verbruggen, *Les Codes commentés. Protection des données à caractère personnel (loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)*, Bruxelles, Larcier, 2011, p. 69.
5. Dictionnaire *Larousse*.
6. *Ibid.*
7. Sur la question de l'obligation d'information en cas de « violation des données » (*data breach*) dans le domaine des communications électroniques, voy. la contribution de K. Rosier, « Vie privée et traitement de données dans le cadre des communications électroniques » dans le présent ouvrage.

La Cour européenne des droits de l'homme considère que la confidentialité et la sécurité sont des éléments essentiels de la protection de la vie privée. Elle a ainsi affirmé que « [l]a législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention (arrêt Z c. Finlande du 25 février 1997, *Recueil des arrêts et décisions* 1997-I, p. 347, § 95) »[1].

7.3.1. Informer le personnel des prescrits légaux en matière de protection des données

Le responsable doit mettre les personnes agissant sous son autorité au courant des prescrits légaux en matière de protection des données[2]. Il doit donc s'assurer que le personnel soit informé des dispositions de la loi vie privée, de son arrêté royal et de toutes autres dispositions pertinentes.

Il peut, par exemple, organiser des formations internes ou distribuer des instructions, sur support papier ou par la voie d'un intranet, destinées à expliquer les principes légaux à respecter.

7.3.2. Veiller à la confidentialité des données

Le responsable du traitement doit veiller à ce que les personnes agissant sous son autorité n'aient la possibilité d'accéder à et d'utiliser que les seules données dont elles ont besoin pour exercer leurs fonctions.[3]

En outre, en présence de données sensibles (données sensibles au sens strict, données relatives à la santé et données « judiciaires »)[4], le responsable doit veiller à ce que les personnes ayant accès à de telles données soient tenues par une obligation légale ou contractuelle de confidentialité[5]. Cela concerne, par exemple, la secrétaire et l'archiviste travaillant pour un centre de santé, une mutuelle, un tribunal ou un cabinet d'avocats, et l'informaticien ayant accès au réseau de ces divers endroits pour en assurer la maintenance.

1. Cour eur. D.H, arrêt M. S. c. Suède, 27 août 1997, req. n° 74/1996/693/885, § 41.
2. Article 16, § 2, 3°, LVP.
3. Article 16, § 2, 2°, LVP.
4. Pour plus de détails sur cette notion, voy. *supra*.
5. Article 25, 3°, de l'arrêté royal.

7.3.3. Veiller à la sécurité des systèmes d'information

Le responsable du traitement doit protéger les informations qu'il a rassemblées contre une curiosité malsaine venant de l'intérieur ou de l'extérieur ou contre des manipulations non autorisées, qu'elles soient de nature accidentelle ou qu'elles soient malintentionnées. Il doit prendre des mesures de différents ordres pour se prémunir contre la perte accidentelle de données, contre la destruction, la modification, l'accès ou tout autre traitement de données accidentel ou non autorisé[1]. Par exemple, en matière de données relatives à la santé, le responsable de traitement devra s'assurer que son personnel médical n'accédera, d'une part, qu'aux données des patients dont il assure le suivi thérapeutique et, d'autre part, qu'aux seules données de ces patients qui lui sont nécessaires dans le cadre du suivi thérapeutique.

Ces mesures sont l'expression de la « politique de sécurité » de l'entreprise, l'administration, l'O.N.G., l'individu, etc., responsables du traitement de données.

a) Mesures organisationnelles

La loi impose ainsi au responsable du traitement de prendre tout d'abord des mesures organisationnelles. Il s'agit de mesures qui sont souvent de bon sens, mais qui, pourtant, dans la pratique observée chez nombre d'avocats, font parfois défaut. Au titre des mesures organisationnelles, on trouve le fait de limiter le nombre de personnes ayant accès aux données, de fermer les locaux où sont localisés les ordinateurs, d'archiver les fichiers dans des armoires fermées à clé, etc. Dans un certain nombre de cas, des systèmes sont très bien protégés au niveau des accès électroniques (mot de passe complexe) mais physiquement sous-protégés dès lors que toute personne circulant dans l'entreprise peut accéder physiquement au serveur et même le subtiliser.

Cette notion de sécurité/confidentialité organisationnelle peut être illustrée à travers l'exemple de l'utilisation des mots de passe pour accéder à un réseau protégé. Il a été constaté que certaines entreprises imposent à leurs employés de changer de mot de passe tous les mois sans pouvoir choisir un mot de passe qu'ils auraient déjà utilisé durant les six derniers mois. Si le principe peut paraître intéressant pour éviter l'usurpation d'identité sur le réseau informatique de la société, cela peut s'avérer, en réalité, une mauvaise stratégie. En effet, on a observé dans certains cas que les employés écrivaient leur mot de passe sur un papier collé à l'ordinateur pour être certains de ne pas l'oublier compte tenu du rythme de changement de mot de passe imposé... Cette organisation au niveau des mots de passe est, dans de telles circonstances, totalement contre-productive dès lors que le système d'information n'est plus protégé de manière efficace. Le responsable du traitement contrevient donc à son obligation de sécurité/confidentialité sans s'en rendre compte.

1. Article 16, § 4, de la loi.

b) Mesures techniques

Le responsable est par ailleurs tenu de prendre des mesures techniques de protection. Ces mesures doivent permettre notamment de protéger les ordinateurs et bases de données contre les virus ou les intrusions (programme anti-virus très fréquemment mis à jour, *firewalls*...). Une mesure technique de protection élémentaire consiste à instaurer des systèmes à accès autorisés via des noms d'utilisateur et mots de passe.

L'élaboration de la politique de sécurité du responsable du traitement peut s'inspirer du modèle proposé par la Commission de la protection de la vie privée. Ce modèle est précisément « destiné à aider le responsable d'un traitement à sécuriser les données à caractère personnel qu'il a l'intention de traiter, également connu sous le nom de "normes minimales de sécurité" ou de "*mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel*" »[1].

Les mesures de référence en matière de sécurité invitent à ce que la politique de sécurité de l'entité qui traite des données comprenne :

- une démarche d'analyse des risques que le traitement présente pour les données à caractère personnel ;
- les priorités retenues et les mécanismes à mettre en place en réponse à cette analyse des risques ;
- le planning de mise en œuvre ;
- les responsabilités et règles organisationnelles mises en place ;
- le processus de gestion des incidents de sécurité ;
- les voies de sensibilisation de l'organisme à cette politique de sécurité ;
- les dispositions retenues afin de maintenir à jour le système de sécurisation une fois installé[2].

c) Niveau de protection adéquat – Obligation de moyens

La loi exige d'atteindre, par ces mesures organisationnelles et techniques, un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels[3].

Le niveau de protection à assurer est fonction notamment de la sensibilité des données traitées et des risques liés à l'utilisation de ces données. Plus les données en cause sont sensibles et les risques pour la personne concernée grands, plus impor-

1. C.P.V.P., « Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel », disponible sur le site de la Commission, à l'adresse http://www.privacycommission.be/fr/lexique/mesures-de-reference.
2. *Ibid.*, p. 2.
3. Article 16, § 4, alinéa 2, de la loi.

tantes seront les précautions à prendre[1]. Si des données relatives à la santé d'une personne sont utilisées en dehors d'un contexte médical, dans le cadre des activités d'un cabinet d'avocats ou d'une assurance, par exemple, on exigera que leur traitement soit encadré de mesures de sécurité sévères.

Le juge qui serait donc amené à analyser cette problématique devra tenir compte de ces différents paramètres en se plaçant au jour de la brèche dans la sécurité.

Il est à noter qu'il s'agit d'une obligation de moyens dans le chef du responsable du traitement qui doit mettre en œuvre tous les moyens raisonnables pour garantir un niveau adéquat de sécurité et de confidentialité des données, compte tenu des différents paramètres énoncés par la loi.

Il est toutefois difficile d'échapper aux conséquences de cette obligation. En effet, la loi vie privée prescrit que « [l]e responsable du traitement est responsable du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi. Il est exonéré de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable »[2]. Le responsable du traitement devra donc prouver qu'un éventuel dommage survenu a été provoqué par un fait qui ne lui est pas imputable. On pourra parler d'une présomption réfragable dès lors que le responsable du traitement est présumé responsable du dommage à moins de démontrer que le fait dommageable ne lui est pas imputable (Cf. *infra*).

---

1. Voy. la Recommandation n° R(97)5 du Comité des ministres du Conseil de l'Europe relative à la protection des données médicales, point 9 : « en matière de données médicales, les mesures techniques et organisationnelles doivent assurer un niveau de sécurité approprié compte tenu d'une part de l'état de la technique et d'autre part de la nature *sensible* des données médicales et de l'évaluation des risques potentiels. Ces mesures doivent faire l'objet d'un examen périodique. Les mesures appropriées devraient être prises visant :
   a) à empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle à l'entrée des installations) ;
   b) à empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports de données) ;
   c) à empêcher l'introduction non autorisée de données dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données à caractère personnel mémorisées (contrôle de mémoire) ;
   d) à empêcher que des systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation) ;
   e) en vue d'une part, de l'accès sélectif aux données et, d'autre part, de la sécurité des données médicales, à assurer que leur traitement soit en règle générale conçu de façon à permettre la séparation :
   - des identifiants et des données relatives à l'identité des personnes ;
   - des données administratives ;
   - des données médicales ;
   - des données sociales ;
   - des données génétiques (contrôle d'accès) ;

   f) à garantir qu'il puisse être vérifié et constaté à quelles personnes ou à quels organismes des données à caractère personnel peuvent être communiquées par des installations de transmission de données (contrôle de la communication) ;
   g) à garantir qu'il puisse être vérifié et constaté *a posteriori* qui a eu accès au système et quelles données à caractère personnel ont été introduites dans le système d'information, à quel moment et par quelle personne (contrôle de l'introduction) ;
   h) à empêcher que, lors de la communication de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport) ;
   i) à sauvegarder les données pour la constitution de copies de sécurité (contrôle de disponibilité) ».
2. Article 15*bis*, alinéas 2 et 3, LVP.

7.3.4. Prévoir certaines garanties en cas de sous-traitance

Il se peut, et c'est vrai dans de nombreux cas, que le responsable du traitement recoure aux services d'informaticiens ou à un service spécialisé dans le traitement des données, pour gérer les aspects techniques des traitements de données (mise en place, alimentation et maintenance de bases de données ; création et hébergement d'un site Internet, services du *Cloud*[1] par exemple). Si les personnes auxquelles on fait appel ne sont pas sous l'autorité directe du responsable du traitement de données, elles seront considérées comme sous-traitants aux yeux de la loi de 1992. Ce sera le cas notamment des sociétés extérieures, mais également de personnes ou d'un département interne à l'entreprise, à l'hôpital ou au cabinet d'avocats, mais ne se trouvant pas sous l'autorité du responsable, celui-ci étant, par exemple, un département et non la société, un service et non l'hôpital, un avocat et non le cabinet.

La loi définit le sous-traitant comme étant « la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données »[2].

Le responsable du traitement peut donc confier tout ou partie du traitement de données à caractère personnel à un sous-traitant. Il ne peut toutefois choisir à la légère son sous-traitant. Il est tenu de le sélectionner sérieusement : la loi ne l'autorise à contracter qu'avec un sous-traitant qui offre des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements de données. Cette responsabilité dans le choix du sous-traitant se trouve donc dans le chef du responsable de traitement qui doit en répondre à la personne concernée.

Par ailleurs, il s'impose aussi de baliser les relations entre responsable du traitement et sous-traitant. Le responsable doit conclure un contrat avec le sous-traitant choisi. Dans ce contrat, le sous-traitant doit obligatoirement s'engager à n'agir que sur instruction du responsable du traitement et à respecter les mesures de protection prises. Le contrat doit également fixer la responsabilité du sous-traitant vis-à-vis du responsable du traitement[3]. Le tout doit être « consigné par écrit ou sur un support électronique »[4].

---

1. Sur le *Cloud Computing* et la protection des données, voy. C. GAYREL, J. GERARD, J.-P. MOINY, Y. POULLET et J.-M. VAN GYSEGHEM, « Data protection in the clouds », *in Computers, Privacy and Data Protection : An Element of Choice*, Dordrecht, Springer, 2011, pp. 377 à 409 ; J.-M. VAN GYSEGHEM, « *Cloud computing* et protection des données à caractère personnel : mise en ménage possible ? », *R.D.T.I.*, 2011, pp. 35 à 50.
2. Article 1er, § 5, de la loi.
3. Article 16, § 1er, de la loi.
4. Article 16, § 1er, 5°, de la loi.

8. Le régime de responsabilité

La loi vie privée prévoit, en son article 15*bis* :

> « Lorsque la personne concernée subit un dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi, les alinéas 2 et 3 ci-après s'appliquent, sans préjudice d'actions fondées sur d'autres dispositions légales.
>
> Le responsable du traitement est responsable du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi.
>
> Il est exonéré de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable. »

Le régime de responsabilité, tel qu'institué par cet article, doit être analysé comme suit.

- Seule la personne concernée peut se prévaloir de cet article 15*bis*. Cela impose donc à la personne concernée de démontrer son statut au risque de voir sa demande déclarée irrecevable.
- La personne concernée doit démontrer, d'une part, son dommage et, d'autre part, un « acte contraire aux dispositions déterminées par ou en vertu de la présente loi ». Par dispositions déterminées « en vertu de la présente loi », l'on comprend également l'arrêté royal du 11 février 2001. Le dommage pourra être tant moral que matériel.
- Ces deux éléments prouvés par la personne concernée, la responsabilité du responsable de traitement est présumée. Il s'agit cependant d'une présomption réfragable ; présomption qui sera cependant assez difficile à renverser. Cette présomption est déduite du fait que la loi tend à protéger la personne concernée et donc à alléger les procédures tendant à faire respecter ses droits. Le caractère réfragable tient au fait que le responsable de traitement peut se dégager de cette présomption à condition de rapporter la preuve de ce que le fait à la source du dommage ne lui soit pas imputable. Il a cependant la charge de cette preuve.

L'on doit attirer l'attention sur le fait que, si le dommage est causé par le sous-traitant, cela ne permettra pas au responsable du traitement de renverser la présomption dès lors que le sous-traitant œuvre pour son compte et sous ses instructions. Il sera assimilé au responsable du traitement qui devait s'assurer que son sous-traitant respecte les principes mis en place par la loi vie privée. Le responsable du traitement pourrait cependant entamer une action récursoire ou en garantie selon les règles

classiques de responsabilité et judiciaires. Cela démontre la nécessité d'un contrat entre les deux[1].

9. Les recours

La loi vie privée a prévu, en son article 14, une compétence exclusive du président du tribunal de première instance pour connaître de « toute demande relative au droit accordé par ou en vertu de la loi, d'obtenir communication de données à caractère personnel, et de toute demande tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte ou, compte tenu du but du traitement, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits, au traitement de laquelle la personne concernée s'est opposée ou encore qui a été conservée au-delà de la période autorisée »[2].

La compétence du président porte donc sur des droits subjectifs accordés à la personne concernée afin de la protéger face au risque de voir des responsables de traitement rechigner face à des demandes d'exercice de ses droits par la personne concernée.

La rédaction de cette disposition soulève cependant un problème dès lors qu'elle date de 1992 et n'a pas été modifiée lors de la transposition de la directive 95/46 en 1998, de sorte que les termes utilisés ne correspondent plus toujours à la rédaction des droits dans sa mouture de 1998.

À titre d'exemple et ainsi que l'explique J. Herveg :

> « la loi du 8 décembre 1992 [dans sa mouture initiale] octroyait à la personne concernée le droit d'obtenir la communication des données qu'un traitement contenait à son sujet et l'article 14 de la loi renvoyait précisément à l'exercice de ce droit. Or, maintenant, ce droit a été étoffé et développé suite à la transposition de la Directive 95/46/CE. Mais la formulation de la compétence matérielle du président sur ce point n'a pas été adaptée à cette évolution. Il s'ensuit une discor-

1. Aux termes de l'article 16, § 1er, de la LVP, « [l]orsque le traitement est confié à un sous-traitant, le responsable du traitement ou, le cas échéant, son représentant en Belgique, doit :
[...]
3° fixer dans le contrat la responsabilité du sous-traitant à l'égard du responsable du traitement ; [...] ».
2. Article 14 LVP. Les pouvoirs du président devant être analysés de manière stricte, il paraît difficile d'utiliser cette voie pour demander réparation d'un dommage découlant d'un infraction à la loi vie privée à moins de considérer cette demande comme un accessoire de la demande principale qui entrerait dans la compétence du président telle que définie par la loi. Voy., à ce sujet, J. Herveg, « La procédure "comme en référé" appliquée aux traitements de données », *Les actions en cessation*, Bruxelles, Larcier, 2006. pp. 215 à 246.

dance formelle entre la définition de cette compétence matérielle et son contenu légal actuel.

[La personne concernée] a donc la possibilité de saisir le Président du tribunal de son domicile ou, à défaut de domicile, de celui du responsable de traitement ou de son siège social.

Cette compétence présidentielle est volontairement limitée par le législateur. Cela signifie donc qu'elle ne peut pas faire l'objet d'extension à, par exemple, une action en responsabilité.

Cela a, pour conséquence, que toute personne concernée ayant subi un dommage et entendant en réclamer réparation devra nécessairement se tourner devant le juge matériellement et territorialement compétent. Les règles classiques du code judiciaire s'appliqueront sans exception »[1].

Cependant et afin de ne pas dénaturer cette action, il faut interpréter l'article 14 dans son contexte actuel et en fonction des droits sur lesquels il porte dans leur nouvelle formulation. Une analyse trop formelle doit être évitée au regard de l'économie du texte. Nous suivons en cela l'enseignement de J. Herveg sur ce point[2]. Il est à noter qu'il s'agit d'une interprétation et non d'une extension de la compétence, ce qui serait à exclure.

Cette compétence présidentielle peut être très intéressante dans certaines matières telles que l'accès à leurs dossiers médicaux par les patients. En effet, la tenue du dossier médical répondant au critère d'application de la loi vie privée et le droit d'accès entrant dans la compétence présidentielle en vertu de l'article 14 de la LVP, le patient pourra l'exercer sans devoir justifier d'aucune urgence comme il devrait le faire en matière de référé classique.

La compétence limitée telle que prévue à l'article 14 implique cependant que toute autre demande devra être portée devant le juge matériellement et territorialement compétent dans le respect des règles du Code judiciaire belge, sans exception.

L'on doit cependant bien constater que le coût d'une procédure est un frein indéniable dans le chef de la personne concernée à porter le débat devant le juge. Il serait donc utile que le droit belge se dote d'un système de « class action » afin de pallier ce problème.

1. J. Herveg, « La procédure "comme en référé" appliquée aux traitements de données », *op. cit.*, p. 223, point 4.
2. J. Herveg, *op. cit.*, p. 224, point 4. Voy. également les pages suivantes pour plus de précisions sur la compétence présidentielle.

Une autre solution serait de voir la Commission de la protection de la vie privée faire usage des pouvoirs qui sont donnés à son président par l'article 32, § 3, de la loi du 8 décembre 1992. En effet, cette disposition lui permet de soumettre au tribunal de première instance tout litige concernant l'application de la présente loi et de ses mesures d'exécution. La Commission remplirait ainsi son rôle de garante du respect de la protection des données à caractère personnel au profit des personnes concernées. Il est, bien entendu, regrettable qu'il ne soit pas fait plus souvent appel à cette compétence[1].

10. La Commission de la protection de la vie privée

Dès sa première mouture, la loi vie privée a établi la Commission de la protection de la vie privée avec un certain nombre de compétences qui n'ont pas été élargies en 1998 lors de la transposition de la directive 95/46, alors que cette dernière en donnait la possibilité au législateur belge.

10.1. Composition

La Commission est un organe du Parlement et ses seize membres – effectifs et suppléants – sont nommés – pour une durée de six ans – par le Parlement sur une double liste présentée par le gouvernement. Cela signifie que le gouvernement choisit les membres qu'il souhaite voir siéger comme commissaires à la Commission. Cela soulève, bien entendu, des questions d'indépendance au regard du poids politique pouvant exister lors de la détermination des candidats qui figureront sur cette double liste. L'on peut également se poser la question de la conformité d'un tel système par rapport à l'article 28.1, alinéa 2, de la directive 95/46 prescrivant que les autorités de contrôle « exercent en toute indépendance les missions dont elles sont investies ». En dépit de son rattachement au Parlement, y a-t-il effectivement une totale indépendance de la Commission de la protection de la vie privée lorsque ses membres sont proposés au Parlement par le pouvoir exécutif ?

La Cour de justice de l'Union européenne a, dans un arrêt du 9 mars 2010, considéré :

> « Compte tenu de tout ce qui précède, il y a lieu d'interpréter l'article 28, paragraphe 1, second alinéa, de la directive 95/46 en ce sens que les autorités

1. Dans le même sens, E. DEGRAVE, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, thèse de doctorat, 2013, à paraître.

de contrôle compétentes pour la surveillance du traitement des données à caractère personnel dans le secteur non public doivent jouir d'une indépendance qui leur permette d'exercer leurs missions sans influence extérieure. Cette indépendance exclut non seulement toute influence exercée par les organismes contrôlés, mais aussi toute injonction et toute autre influence extérieure, que cette dernière soit directe ou indirecte, qui pourraient remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel »[1].

Il n'est pas exclu qu'une « obéissance anticipée »[2] de la Commission à l'égard du pouvoir politique s'installe[3].

La Cour de justice de l'Union européenne est allée plus loin en considérant que l'indépendance fonctionnelle de l'autorité de contrôle « ne suffit pas, à elle seule, à préserver ladite autorité de contrôle de toute influence extérieure »[4].

Elle complète cela en considérant que « l'indépendance requise au titre de l'article 28, paragraphe 1, second alinéa, de la directive 95/46 vise à exclure non seulement l'influence directe, sous forme d'instructions, mais également, [...], toute forme d'influence indirecte susceptible d'orienter les décisions de l'autorité de contrôle »[5].

La Commission de la protection de la vie privée belge répond-elle réellement à cette obligation d'absence de toute forme d'influence ?

Par ailleurs, au niveau de la composition, il faut relever la parité linguistique entre les membres d'expression française et flamande ; parité qui se retrouve au sommet de la Commission dès lors que, lorsque le président – obligatoirement un magistrat détaché – est d'expression flamande, le vice-président est d'expression francophone, et vice versa.

En pratique, la commission se réunit à seize membres et les décisions sont prises par consensus.

1. C.J.U.E., 9 mars 2010 (Commission c. Allemagne), C-518/07, point 30.
2. C.J.U.E., 9 mars 2010, préc., point 36.
3. Voy., à ce sujet, C. GAYREL, « Chronique de jurisprudence : Cour de Justice de l'Union européenne, Tribunal de première instance et Tribunal de la fonction publique européenne », *R.D.T.I.*, 2012, n^{os} 48 et 49, p. 96, point 140.
4. C.J.U.E., 16 octobre 2012 (Commission européenne c. République d'Autriche), C-614/10, point 42.
5. C.J.U.E., 16 octobre 2012, préc., point 43.

10.2. Compétences

La Commission a une *compétence d'avis* par rapport à « toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre de la [loi vie privée], ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel »[1].

La loi lui a également donné une *compétence de recommandation* « sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre de la présente loi, ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel »[2].

Au niveau des droits individuels des personnes concernées, la Commission *peut être saisie par voie de plainte* qu'elle instruira conformément à son règlement d'ordre intérieur.

Dans le cadre de cette compétence, elle jouera un rôle de conciliateur et tentera d'arriver à une solution compatible avec les principes relatifs à la protection des données à caractère personnel. En cas d'absence de conciliation, elle émettra un avis motivé qu'elle pourra accompagner de recommandations également motivées à l'intention du responsable du traitement. Une copie de cet avis ou cette recommandation est communiquée au plaignant, à toute partie à la cause, ainsi qu'au SPF Justice. Il est à noter que l'identité du plaignant n'est pas révélée à moins que « l'examen de la plainte le requière et si le plaignant y a consenti »[3]. Le Règlement d'ordre intérieur de la Commission prévoit également que, « si la divulgation de l'identité du plaignant est nécessaire pour pouvoir examiner la plainte mais que le plaignant ne donne pas son consentement à cet effet, la plainte est classée sans suite »[4]. Si ces recommandations ne sont pas suivies, elle n'aura pas cependant la compétence d'interdire le traitement, mais pourra ester en justice pour faire respecter les intérêts de la personne concernée sur pied de l'article 32, § 3, de la LVP.

La Commission procède également à un **contrôle** externe du traitement de données à caractère personnel par le biais de la déclaration en s'assurant du ou des traitements par rapport aux principes de la loi vie privée. À la suite de ce contrôle, elle pourra demander toute explication qu'elle estime nécessaire.

1. Article 29, § 1er, LVP.
2. Article 30, § 1er, LVP.
3. Article 26 du Règlement d'ordre intérieur de la Commission de la protection de la vie privée.
4. Article 26 du Règlement d'ordre intérieur de la Commission de la protection de la vie privée.

La Commission peut également :

- mener des contrôles de sa propre initiative ou à la suite d'une déclaration, d'une demande d'information ou d'une plainte[1] ;
- mener des inspections avec l'aide, ou pas, d'expert tant à la suite d'un contrôle ou de manière préventive[2].

Elle n'a aucun pouvoir de sanction, mais peut, par contre, ester en justice et transmettre un dossier au parquet, compétences qui ne sont guère – pour ne pas dire pas du tout – exercées.

10.3. Comités sectoriels

Si les pouvoirs de la Commission n'ont guère évolué depuis 1992, la grande nouveauté est intervenue en 2003. En effet, le législateur a créé, au sein de la Commission, les comités sectoriels. Cette modification de la loi s'est accompagnée, dans les matières relevant de l'intervention des comités sectoriels, de la transformation de la déclaration en autorisation pour certaines matières.

Les comités sectoriels sont au nombre de six étant le comité sectoriel du Registre national, celui pour l'autorité fédérale, ceux de la sécurité sociale et de la santé, de surveillance statistique, de la Banque-carrefour des entreprises et de surveillance Phenix.

Chaque comité est constitué de membres de la Commission et des représentants du terrain. Ces comités donnent des autorisations pour certains traitements.

Nous ne nous attarderons pas plus longuement sur ces comités dès lors qu'ils seront analysés dans la partie du présent ouvrage dédiée aux traitements des données à caractère personnel dans le secteur public.

11. Sanctions pénales

Partant du principe qu'une loi sans sanction est une loi qui sera tôt ou tard violée, le législateur a prévu, au chapitre VIII de la LVP, des sanctions pénales en cas d'infractions à certaines dispositions de cette loi.

1. Article 38, alinéa 1er, du Règlement d'ordre intérieur de la Commission.
2. Article 38, alinéa 2, du Règlement d'ordre intérieur de la Commission.

Ces dispositions qui font l'objet d'une protection pénale touchent, entre autres, à la confidentialité et à la sécurité, aux conditions de traitement, au droit d'accès et à la déclaration à la Commission de la vie privée.

Les sanctions vont de l'amende à la « confiscation des supports matériels des données à caractère personnel formant l'objet de l'infraction, tels que les fichiers manuels, disques et bandes magnétiques, à l'exclusion des ordinateurs ou de tout autre matériel, ou [à] l'effacement de ces données »[1] en passant par la publication du jugement soit dans son intégralité, soit en extraits dans un ou plusieurs journaux.

Cette dernière peine paraît, en réalité, la plus efficace dans le chef d'entreprises qui n'auraient aucune peine à payer l'amende dont le coût aurait même été intégré dans leurs analyses de coûts/bénéfices. En effet, une entreprise pourra faire une balance entre le bénéfice que rapporterait un traitement même illégal par rapport au coût que générerait le respect de la loi. On doit entendre le terme « coût » au sens large et non uniquement financier. L'on se rend alors compte que l'amende importe peu aux entreprises fonctionnant sur ce type de scénario.

Par contre, la publication du jugement pourrait impacter les responsables du traitement indélicats de manière beaucoup plus significative. Le juge ne devrait donc pas hésiter à utiliser cette sanction.

L'on pourrait également imaginer la création d'une liste noire des responsables du traitement indélicats en situation de récidive. Cela permettrait aux personnes concernées d'être plus informées encore et donc mieux protégées.

Une autre critique que nous pouvons à nouveau formuler à l'égard du régime belge est la réticence des personnes concernées à porter plainte au regard du coût en temps et argent qu'une telle procédure engendrerait. Il s'agit du même problème que celui relevé en matière civile bien qu'il soit atténué par le fait que, dans le cadre de la procédure pénale, le parquet et/ou le juge d'instruction instruit le dossier. Mais encore faut-il que la protection des données à caractère personnel ne soit pas reléguée au rang des priorités secondaires…

Ce problème pourrait encore être atténué dès lors que la loi *impose* à la Commission de la protection de la vie privée de dénoncer au procureur du Roi les infractions dont elle a connaissance, ce qu'elle ne fait malheureusement pas davantage que la démarche qui lui est ouverte sur le plan civil, contrevenant ainsi à la loi vie privée. Cette obligation de dénonciation, sous réserve d'exceptions légales, découle de la formulation même de l'article 32, § 2, de la LVP qui stipule que « la Commission dénonce au procureur du Roi les infractions dont elle a connaissance »[2]. Elle n'a

1. Article 31 LVP.
2. Article 32, § 2, LVP.

donc pas le choix et, cependant, elle ne se soumet pas à ce prescrit légal. Pourtant, par cette possibilité de dénonciation au parquet, la Commission permettrait une meilleure protection des personnes concernées.

La peur du gendarme a ses limites et, quand le temps de la médiation chère à la Commission est terminé, il faut, à un certain moment, passer aux sanctions. Il en va de la crédibilité même de l'institution.